TAC Xenta®

Engineering TAC Xenta 527

t.a.c®

TAC Xenta®

Engineering TAC Xenta 527

t.a.c®

Copyright © 2004 TAC AB. All rights reserved.

This document, as well as the product it refers to, is only intended for licensed users. TAC AB owns the copyright of this document and reserves the right to make changes, additions or deletions. TAC AB assumes no responsibility for possible mistakes or errors that might appear in this document.

Do not use the product for other purposes than those indicated in this document.

Only licensed users of the product and the document are permitted to use the document or any information therein. Distribution, disclosure, copying, storing or use of the product, the information or the illustrations in the document on the part of non-licensed users, in electronic or mechanical form, as a recording or by other means, including photo copying or information storage and retrieval systems, without the express written permission of TAC AB, will be regarded as a violation of copyright laws and is strictly prohibited.

Trademarks and registered trademarks are the property of their respective owners. Microsoft® and Windows® are registered trademarks of The Microsoft Corporation.

Trademarks and registered trademarks are the property of their respective owners.

TAC Vista®, TAC Menta®, TAC Xenta® and TAC I-talk® are registered trademarks of TAC AB.

Contents

INTRODUCTION

1 About this Manual 9
1.1 Structure ... 9
1.2 Typographic Conventions ... 10
1.3 Prerequisites ... 10
1.4 How to Use this Book ... 11

GETTING STARTED

2 Configuration Instructions 15
2.1 Preparing to Configure the Xenta 527 ... 15
2.2 Setting the IP Address for the TAC Xenta 527 ... 15
2.3 Connecting the Xenta 527 to Your Network ... 17
2.4 Using a Proxy Server ... 18
2.5 Working With Firewalls ... 19

3 Logging Into the TAC Xenta 527 21
3.1 Connecting Through a Web Browser ... 21
3.2 Using a Self-Signed Certificate ... 21

4 Setting Up I/NET Communications 25
4.1 Defining I/NET Host IP Addresses ... 25
4.2 Defining Host Masks ... 27

5 Securing the Web Server 29
5.1 Setting up Password-protected User Accounts ... 29
5.2 Assigning User Access Rights ... 31
5.3 Logging Failed Login Attempts ... 32
5.4 Extending Time Between Failed Login Attempts ... 33
5.5 Configuring Secure Socket Layer Connections ... 33
5.6 Preventing Remote Configuration Clients from Altering Parameters ... 36

6 Creating Web Pages with XBuilder 39
6.1 Using XBuilder ... 39
6.2 Creating a Project That Will Include I/NET Items ... 40
6.3 Converting and Importing I/NET SAV Files ... 42
6.4 Updating Your Project with New I/NET SAV Files ... 44
6.5 Displaying Dynamic I/NET Alarms and Events from Web Pages ... 45
6.6 Using I/NET Point Signals ... 47
6.6.1 Mapping I/NET Point Signals to Web Pages ... 47
6.6.2 Mapping I/NET Point Signals to Graphic Pages ... 49

6.7 Using I/NET Page Links 54
6.7.1 Linking an I/NET Trend Log to a Graphic Page 54
6.7.2 Linking an I/NET Time Schedule to a Graphic Page 58
6.8 Using the Find Function 62

REFERENCE

7 I/NET Objects in XBuilder 67
7.1 Network Objects 68
7.2 Point Signals 68
7.3 Page Links 69

8 DCU-to-XML Conversion Utility 73
8.1 Launching the Utility from an Explorer Window 73
8.2 Running the Utility from the Command Line 74

9 History Logs 77
9.1 Occurrences of I/NET System and Web Server Alarms and Events 77
9.2 Records of Individuals Who Modified an Alarm Status 77

10 Storing Data on the Xenta 527 79
10.1 Data Limits 79
10.2 Web Server Data 79
10.3 Protecting Stored Data 79
10.3.1 Maintaining Data During Power Interruptions 79
10.3.2 Backing Up and Restoring Data 79

APPENDIX

A Frequently Asked Questions (FAQs) 85

B Troubleshooting 87

Index 91

Introduction

1 About this Manual

1 About this Manual

This manual describes the configuration and operation of the TAC Xenta 527. For information on supporting products, please refer to the manual for the product in question.

The TAC Xenta 527 provides the same capabilities as the Xenta 511, as well as additional features that support the use of I/NET systems. The focus of this manual is to explain the features that are unique to the Xenta 527. For an explanation of the features that are common to both the Xenta 511 and Xenta 527, refer to the Xenta 511 documentation.

Note

We are continuously improving and correcting our documentation. This manual may have been updated.

Please check our Docnet site at www.tac.com for the latest version.

1.1 Structure

The manual is divided into the following parts:

- **Introduction**
  The Introduction section contains information on how this manual is structured and how it should be used to find information in the most efficient way.
- **Getting Started**
  The Getting Started section contains a step-by-step description of how to engineer or carry out different tasks. It also gives you guided instructions on how to complete a sample project. If you want more information, see the corresponding chapter in the Reference section of the manual.
- **Reference**
  The Reference section contains more comprehensive information about various parts of the Getting Started section. It also provides you with information on alternative solutions not covered by the Getting Started section.

1.2 Typographic Conventions

Throughout the manual the following specially marked texts may occur.

Warning

Alerts you that failure to take, or avoid, a specific action might result in physical harm to you or to the hardware.

Caution

Alerts you to possible data loss, breaches of security, or other more serious problems.

Important

Alerts you to supplementary information that is essential to the completion of a task.

Note

Alerts you to supplementary information.

Tip

Alerts you to supplementary information that is not essential to the completion of the task at hand.

1.3 Prerequisites

To be able to profit from the contents in this manual, you are recommended to read the following manuals:

- *TAC Xenta® 511 and 911 Handbook*, document no. 0-004-7870-0
- *Engineering TAC Xenta 511*, document no. 0-004-7845-3
- *Operating TAC Xenta 511*, document no. 0-004-7846-1.

1.4 How to Use this Book

This document follows a standard style indicating keystrokes, cursor movement, navigation, and data entry. TAC software is intended to be used primarily with a mouse. However, you may use keyboard equivalents as indicated below.

Filenames

Filenames appear in this manual as they appear on the screen of your computer. To further identify them as files, they appear as uppercase, italicized letters with any file extensions included. For instance, the configuration file used by your computer upon start up is shown as *CONFIG.SYS*.

Menu Commands

Menu selections are shown in bold font with initial capitalization as in **Edit**. A menu item with the arrow symbol (▸) indicates another menu level.

Keystrokes

Keystrokes are shown in bold surrounded by square brackets. For example, the Y key is shown as **[Y]**, and the Enter key is shown as **[Enter]**.

Certain standard keys are used within the application to perform certain system functions within editors, message boxes, etc. These are the **[Enter]**, **[Esc]**, **[Tab]**, and Up and Down Arrow keys.

- **[Enter] Key** — Use this key to accept or activate a function, typically a highlighted button.
- **[Esc] Key** — Use this key to cancel an action or editor. You may use the [Esc] key to back up from successive levels of windows until you return to the main application window.
- **[Tab] Key** — Use this key to cycle through the available active buttons or entry fields in an editor or screen.
- **Up/Down Arrows** — Use these keys to move the highlighted selection from one item to another in the various list, drop-down, and combo boxes found in the editors.

Getting Started

2 Configuration Instructions

3 Logging Into the TAC Xenta 527

4 Setting Up I/NET Communications

5 Securing the Web Server

6 Creating Web Pages with XBuilder

2 Configuration Instructions

2.1 Preparing to Configure the Xenta 527

Before you begin configuring the TAC Xenta 527, take time to gather crucial network information. First determine whether *fixed IP address* or *DHCP* (Dynamic Host Configuration Protocol) will be used. If DHCP is used, the TAC Xenta 527 IP address will be assigned by the DHCP server.

Gather the following additional information:

- IP address (If fixed; e.g. 172.20.4.21):
- Subnet mask (If fixed; e.g. 255.255.0.0):
- Default Gateway (e.g. 172.20.2.100):
- DNS (e.g. 192.165.248.22):
- Web site name:
- Domain name:
- Host name:

2.2 Setting the IP Address for the TAC Xenta 527

In order to set the IP Address for the TAC Xenta 527, you will need to connect a serial cable between the Xenta 527 and your PC workstation. You can then use a terminal emulator such as Hyperterminal within Windows to communicate with the Xenta 527.

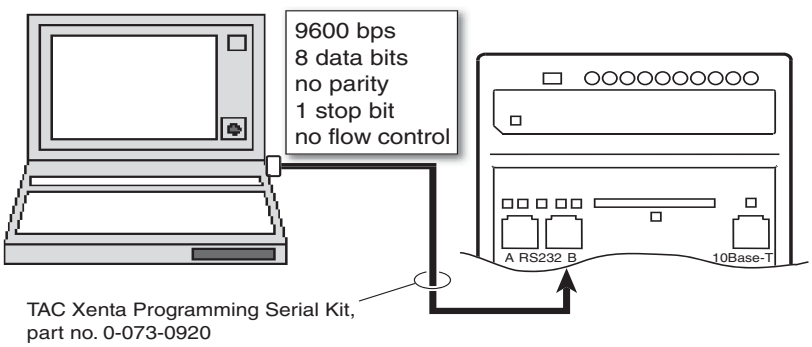


Fig. 2.1: Using a Terminal Emulator to Communicate with the TAC Xenta 527

1 Connect a serial cable between the PC and the Xenta 527 RS232 B port.

2 Within Windows, start a terminal emulator such as Hyperterminal.

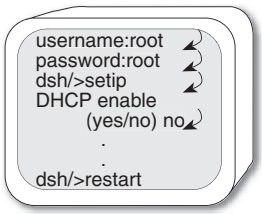


Fig. 2.2: Assigning the IP address using Hyperterminal

3 Log into the TAC Xenta 527 by entering a valid user name and password.

4 Type setip to start the configuration script.

5 Answer the DHCP enable question as follows:

- No - Choose this answer if you will assign a static IP address.
- Yes - Choose this answer if you will allow the system to assign the IP address.

6 Depending on the DHCP setting you chose, continue as follows:

- If DHCP Enable = No, enter the following:
  - IP address
  - Subnet mask
- If DHCP Enable = Yes, enter the following:
  - Default Gateway
  - DNS
  - Web site name
  - Domain name
  - Host name

7 Change root password (immediately or later, using passwd).

8 “Do you want to restart the IP interface?”

- Answer Yes to make the changes effective immediately
- Answer No to make the changes effective after the next 527 restart.

9 Exit by typing **lo** (log out) and pressing **[Enter]**.

2.3 Connecting the Xenta 527 to Your Network

The TAC Xenta 527 integrates with I/NET and Vista networks by communicating with these systems across the Ethernet. The following figure shows an example network configuration.

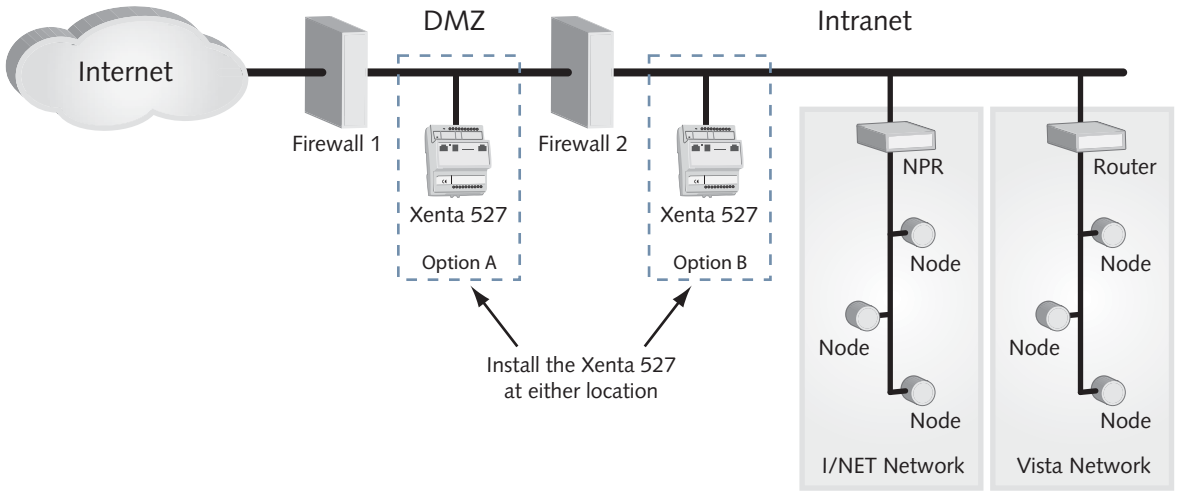


Fig. 2.3: Network Location Options for the Xenta 527

In order for the Xenta 527 to successfully establish communications with your building control systems, certain network criteria must be met. More specifically, the ports required for proper communication with these systems must be open and available to the Xenta 527. The TAC Xenta 527 uses the following communication ports:

- Port 80 (http access)
- Port 443 (https access)
- Port 20/21 (FTP access)
- Port 25 (SMTP access)
- Port 80 (Status Viewer, Alarm Viewer and Graphics Viewer)
- Port 1068 (LTA for Vista)
- Port 161 (snmp access)
- UDP Port 50069 (I/NET system access)

Note

You have the option of changing the HTTP, HTTPS, and Dynamic variables communication Port settings. Refer to page 89 in Chapter B, “Troubleshooting”, for more information.

Connect the Xenta 527 to your network at the desired location. If necessary, configure the network’s proxies/firewalls to allow for proper communication. Refer to “Using a Proxy Server” and “Working With

Firewalls" later in this chapter for general information about these devices.

The figure above shows an example network and the location options for the Xenta 527. Each location is described below.

Explanation of Option A:

The first location (see Fig. 2.3, option A) shows the Xenta 527 installed in the DMZ between two firewalls (be aware that this may be logically two firewalls but physically only one piece of hardware). This location requires the following configuration:

- **Firewall 1:** For security reasons, you may only want to open ports 80 and 443 from the internet. This is all that is necessary for internet access to the Xenta 527's web interface.
- **Firewall 2:** Open ports 20, 21, 25, 80, 161, and 443 from the intranet side. Also open port 1068 and UDP port 50069 from the DMZ side to allow the Xenta 527 to communicate with I/NET and Vista networks.

Explanation of Option B:

The second location (see Fig. 2.3, option B) shows the Xenta 527 installed on the network with no firewall between it and the building control systems. This location requires that both firewalls allow traffic through ports 80 and 443. The other ports are not required to be open on either firewall since the Xenta 527 is installed at a network location that allows it to communicate directly with I/NET and Vista networks.

2.4 Using a Proxy Server

A proxy server is a server that sits between a client application, such as a web browser, and a target server. The proxy server intercepts all requests to the target server. Proxy servers have two main purposes, as described below.

Improve Performance:

Proxy servers can be configured to improve client request response time by saving the results of all requests for a certain amount of time. If a client requests information that has been saved, the proxy server can respond to the client request quickly with the stored information.

Filter Requests:

A proxy server can modify a client request before sending it on to the server. When the server responds, the response also passes through the proxy before it is forwarded on to the client. The proxy can modify the headers in this response.

By intercepting and translating network transactions, a proxy server can:

- Protect the client by monitoring potentially dangerous transactions.
- Enable the client to communicate using protocols that might not be implemented by the client software.
- Act as a gateway between a private network and a public network.

2.5 Working With Firewalls

A firewall is a system designed to prevent unauthorized access to or from a private network. Firewalls can be implemented in both hardware and software, or a combination of both. Firewalls are frequently used to prevent unauthorized Internet users from accessing private networks connected to the Internet, especially intranets. All messages entering or leaving the intranet pass through the firewall, which examines each message and blocks those that do not meet the specified security criteria.

There are several types of firewall techniques:

- **Packet filter:** Looks at each packet entering or leaving the network and accepts or rejects it based on user-defined rules. Packet filtering is fairly effective and transparent to users, but it is difficult to configure. In addition, it is susceptible to IP spoofing.
- **Application gateway:** Applies security mechanisms to specific applications, such as FTP and Telnet servers. This is very effective, but can impose a performance degradation.
- **Circuit-level gateway:** Applies security mechanisms when a TCP or UDP connection is established. Once the connection has been made, packets can flow between the hosts without further checking.
- **Proxy server:** Intercepts all messages entering and leaving the network. The proxy server effectively hides the true network addresses.

In practice, many firewalls use two or more of these techniques in concert.

3 Logging Into the TAC Xenta 527

3.1 Connecting Through a Web Browser

1 Start Internet Explorer.

2 Type the Xenta 527's IP address in the address field in the browser and click the **Go** arrow.

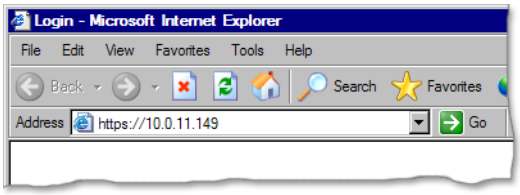


Fig. 3.1: Typing the Xenta 527's IP Address

3.2 Using a Self-Signed Certificate

If you are using a self-signed certificate (i.e. a self-signed certificate has been created in the XBuilder project and sent to the target), you will see the Security Alert dialog when you connect to the Xenta 527. This dialog will appear each time you connect to the Xenta 527, unless you install the certificate on your system.

Fig. 3.2: Security Alert

1 Proceed by performing one of the following actions:

- If you trust the content and would like to proceed *without* installing the self-signed certificate, click **Yes** and proceed with Step 3, below.

- If you do not trust the content and would like to abort the connection, click **No**. In this case, do not perform any of the following steps.
- You can view, and optionally install, the self-signed certificate by clicking **View Certificate**. If you wish to install the certificate, proceed with Step 2, below.

2 If you are viewing the certificate and wish to install it, perform the following steps:

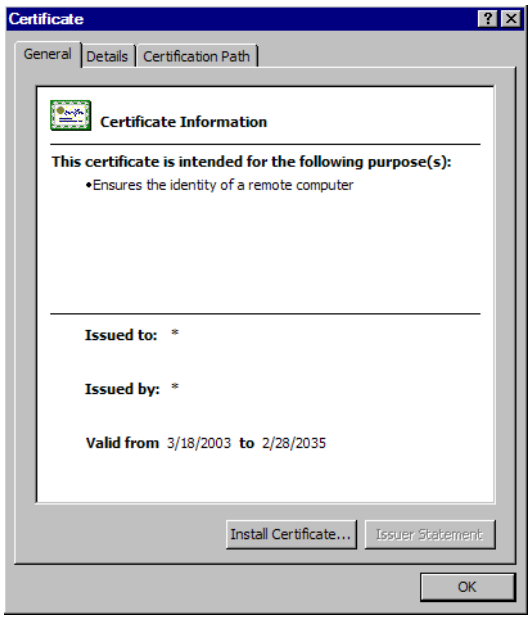


Fig. 3.3: Viewing the Self-signed Certificate

a Click **Install Certificate**. The **Install Certificate Wizard** opens.

b Click **Next** in each dialog presented by the wizard. We recommend that you use the default settings. When the final dialog appears, click **Finish** to end the wizard.

c Close and restart the web browser.

d In the web browser's address field, type the Xenta 527's IP address.

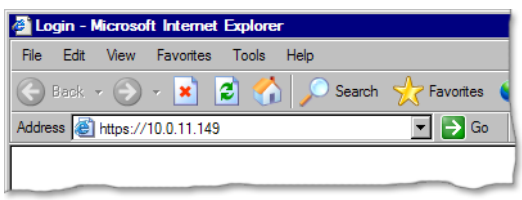


Fig. 3.4: Typing the Xenta 527's IP Address

Since the certificate is installed, no security alert dialog will appear when you connect to the Xenta 527. Proceed to Step 3.

3 Log in as the System Administrator by performing the following steps:

Fig. 3.5: Logging In

a The root account is the system administrator. Therefore, enter a Username of *root*.

b Enter the password for the root account. The default password for this account is *root*.

c Click **Login**.

Being logged in as the System Administrator, you are now able to set up I/NET communications and create user accounts.

4 Setting Up I/NET Communications

4.1 Defining I/NET Host IP Addresses

In order for the TAC Xenta 527 to communicate with I/NET devices from across an Ethernet, it must first obtain the IP addresses of remote I/NET hosts from at least one I/NET reference host. A Reference Host is any I/NET workstation or NetPlus Router that serves as a source of IP addresses. Any host workstation or NetPlus Router attached to an Ethernet LAN can be used as a Reference Host.

I/NET host IP addresses may be entered from a web page or from the console, or downloaded as part of an XBuilder project. You can also assign an I/NET host number to the Xenta 527 while you are defining IP addresses.

From a Web Browser:

1 Expand the INet section of the navigation tree as shown in the following figure and select **Configuration Profile** to define Host IP addresses.

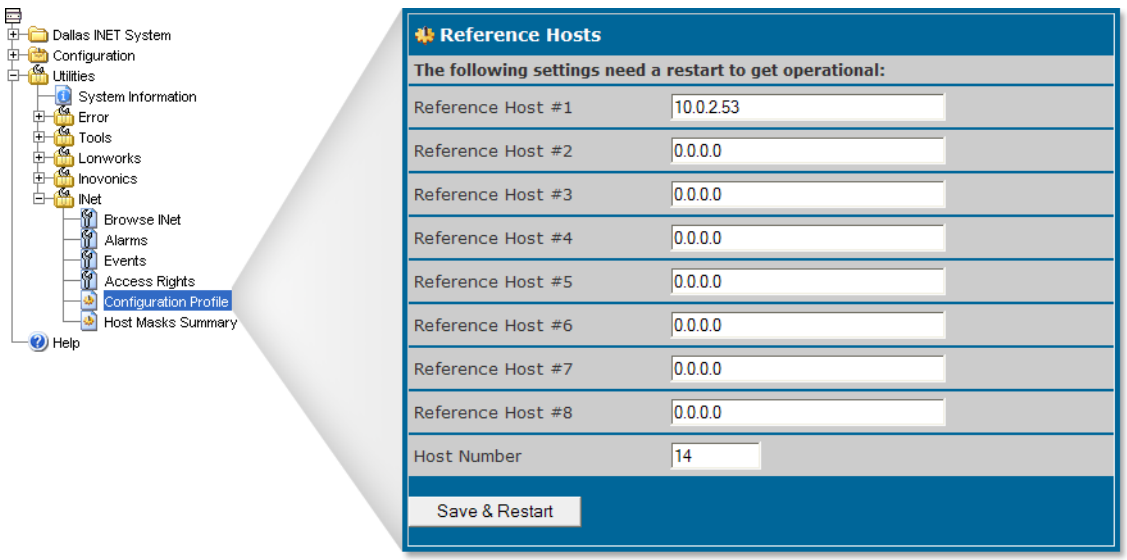


Fig. 4.1: Defining Reference Host IP Addresses from a Web Browser

2 Define an IP Address for each reference host. If you define less then eight reference hosts, set the unused fields to "0.0.0.0".

3 Assign an I/NET host number to the Xenta 527. This can be any number from 1 to 63. Make sure that the number you define is unique among all hosts on the I/NET network.

From a Console Window:

In order to enter host IP addresses from a console window, you will need to connect a serial cable between the Xenta 527 and your PC workstation. You can then use a terminal emulator such as Windows Hyperterminal to communicate with the Xenta 527. If necessary, refer to Fig. 2.1 (*page 15*) to view a typical serial cable connection.

1 After logging into the Xenta 527, begin entering host IP addresses by typing **`inethost`** at the command line (see the figure below).

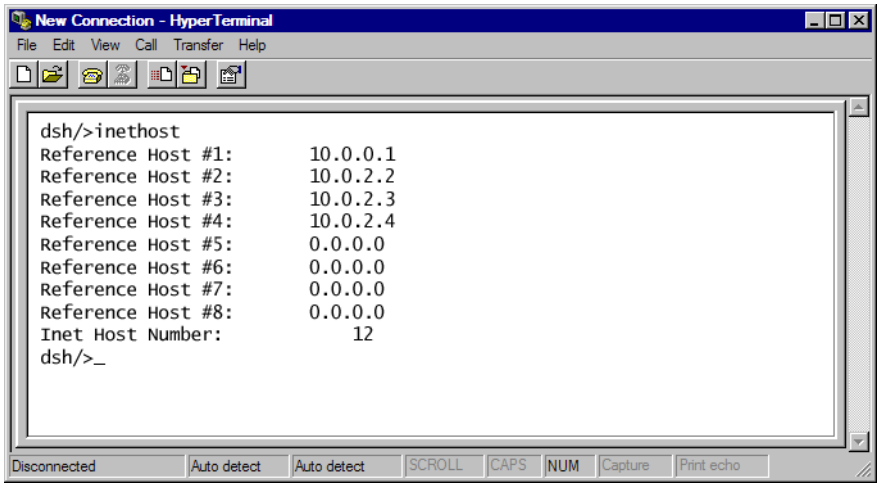


Fig. 4.2: Entering Host IP Addresses from a Console Window

The **`inethost`** command is only available from the console. The addresses you define enable the Xenta 527 to communicate with one or more reference hosts. Up to eight reference host IP addresses can be defined. Set any unused reference hosts to "0.0.0.0".

2 Assign an I/NET host number to the Xenta 527. This can be any number from 1 to 63. Make sure that the number you define is unique among all hosts on the I/NET network

From an XBuilder Project:

In Project mode, the I/NET network is imported into XBuilder. When you transfer the compiled project to the Xenta 527, any Host IP addresses that you have defined from a web browser or from a console window will be overwritten.

1 In XBuilder, open or create a project that uses the X527 project template. For instructions on how to create a project, refer to “Creating a Project That Will Include I/NET Items” on page 40.

2 In the Network pane of XBuilder, expand the **IP Backbone** item and highlight the **INET** object.

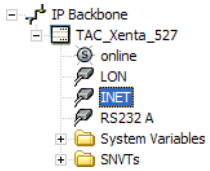
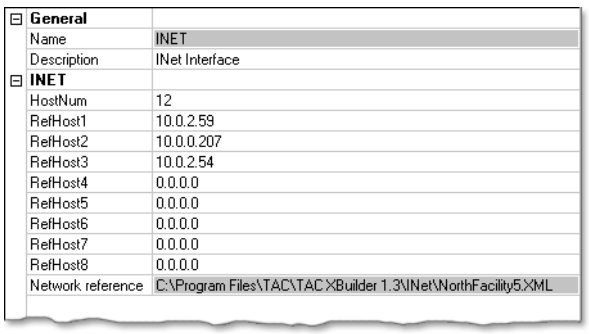


Fig. 4.3: The INET Object in XBuilder

3 In the parameters for the **INET** object, define IP addresses for up to eight reference hosts. Set any unused reference hosts to "0.0.0.0".



General	
Name	INET
Description	INet Interface
INET	
HostNum	12
RefHost1	10.0.2.59
RefHost2	10.0.0.207
RefHost3	10.0.2.54
RefHost4	0.0.0.0
RefHost5	0.0.0.0
RefHost6	0.0.0.0
RefHost7	0.0.0.0
RefHost8	0.0.0.0
Network reference	C:\Program Files\TAC\TAC XBuilder 1.3\INet\NorthFacility5.XML

Fig. 4.4: Setting IP Addresses from XBuilder

4 Define an I/NET host number for the Xenta 527. This can be any number from 1 to 63. Make sure that the number you define is unique among all hosts on the I/NET network.

5 Compile the project and download it to the TAC Xenta 527.

4.2 Defining Host Masks

Masks are part of a filtering system I/NET uses to route messages, alarms, and data to host workstations. The TAC Xenta 527 also makes use of masks in order to receive alarm and event information from the I/NET system.

The masks you define in the Xenta 527 are sent to remote hosts in the I/NET system, allowing them to determine whether to send messages to the Xenta 527. These remote hosts (workstations and NetPlus Routers) compare this mask information to the mask information that accompanies each message received from an I/NET controller. If this comparison results in a match, the message is routed from the remote host to your Xenta 527.

1 Expand the INet section of the navigation tree as shown in the following figure and select **Host Masks Summary** to define Host IP addresses.

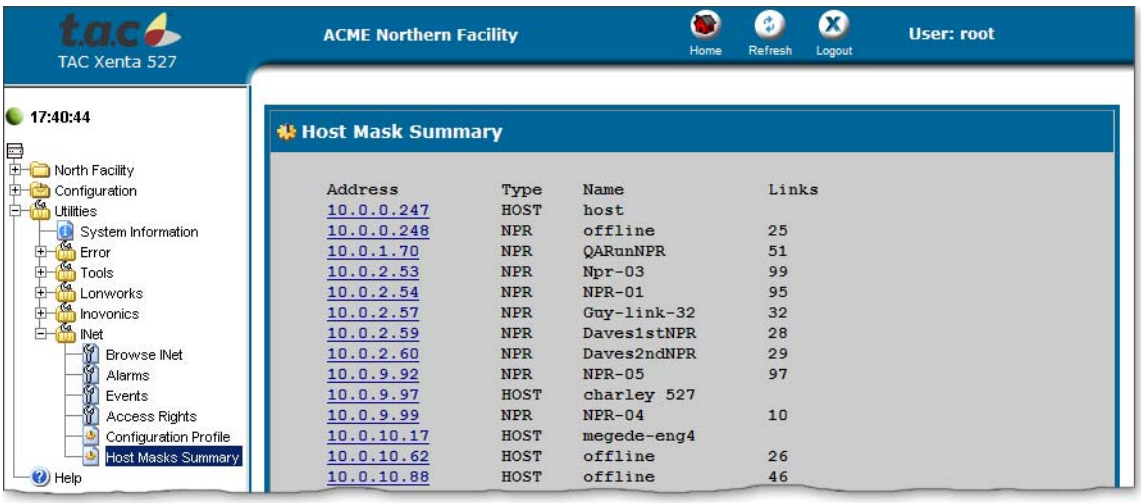


Fig. 4.5: Defining Host Routing Masks

2 In the Host Mask Summary, click on a host IP address to set its routing masks. The Host Routing Mask Editor opens.

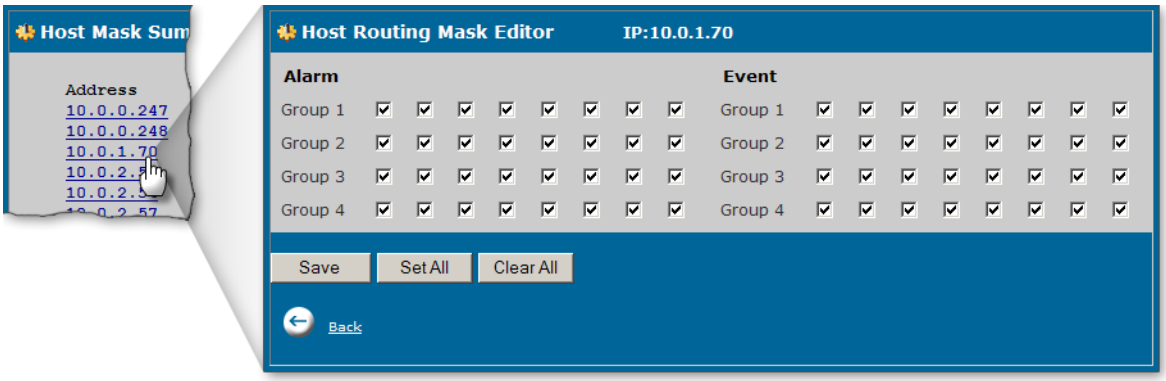


Fig. 4.6: Launching the Host Routing Mask Editor

3 Activate (☑) or deactivate (☐) masking positions as necessary. You can define up to 32 different masks for alarms, and another 32 different masks for events. The masks you define in this editor are sent to the selected host, allowing it to determine whether to send messages to the Xenta 527.

If necessary, you can use the **Set All** and **Clear All** buttons to speed up the selection process.

4 With all masks properly defined, click **Save** to accept your settings.

5 Repeat these steps as necessary to define masks for other I/NET hosts.

5 Securing the Web Server

5.1 Setting up Password-protected User Accounts

The TAC Xenta 527 is a multi-user system that allows each user to have access to specific parts of the system. The authorization level of the different users can only be set by the system administrator, the “root” user. For security reasons, you should change the password for the root user while you are commissioning the Xenta 527.

Read and read/write authorization is assigned at the directory level. The rights are set recursively, which means that subdirectories get the same access level as the folder in which they are located.

The Xenta 527 uses the Xenta 511’s method for assigning read or read/write rights to objects. However, the Xenta 527 also allows you to assign user access rights to I/NET links and stations.

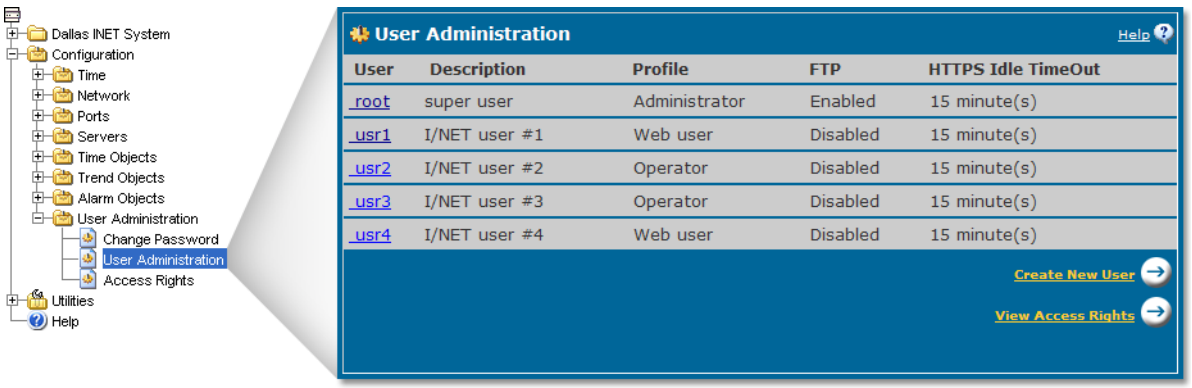


Fig. 5.1: User Administration

In User Administration you can create a new user by performing the following steps:

1 Select **Create New User**. The Create User screen displays (see the figure on the next page).

2 In the **User Details** section, enter the user’s name and a brief description of this user account. The four first characters of the name are used as a signature in connection with I/NET events and alarms.

3 In the **Password Options** section, define a password for the new user.

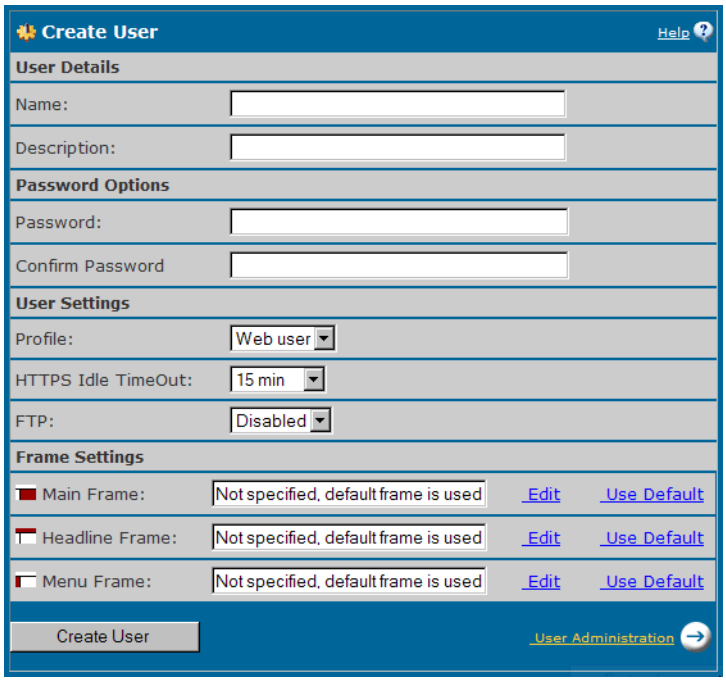


Fig. 5.2: Creating a New User

4 Use the **User Settings** section to customize the new account. The following options are available:

- **Profile** – Assign one of the following profiles to this user:
  - Web User - The web user has minimal access to the system. This user cannot browse the I/NET system, control I/NET points, access I/NET trend logs, or access I/NET time schedules.
  - Operator - The operator has access to all viewers and whatever is needed to supervise the operation of the building. By default, the operator has read/write permission in the relevant parts of the system, and is able to handle all alarms.

  A third setting, called Administrator, also exists, but this setting is restricted to the root user account. Refer to the Xenta 511 documentation for more information about these options.
- **HTTPS Idle TimeOut** – This setting determines what duration of user inactivity will cause automatic user logout. You can choose a setting from 15 minutes to 24 hours.
- **FTP** – Choose whether or not this user will have the ability to transfer files to and from the Xenta 527 using FTP. Be aware that FTP is not a secure method of communication. Passwords, etc. can easily be intercepted.

5 Use the **Frame Settings** section to link customized web pages to this user account. Using this feature, you can design and specify individual web pages for different users. Refer to the Xenta 511 documentation for further information about this feature.

6 Click the **Create User** button to create the new user account.

5.2 Assigning User Access Rights

An I/NET user can receive access rights to I/NET using the I/NET Access Rights Explorer. Expand the navigation tree as shown in the following figure and select **Access Rights**. Initially, the Link layer of your I/NET system is displayed. You can assign user access rights at this level, and penetrate down to the next layer by selecting the appropriate link.

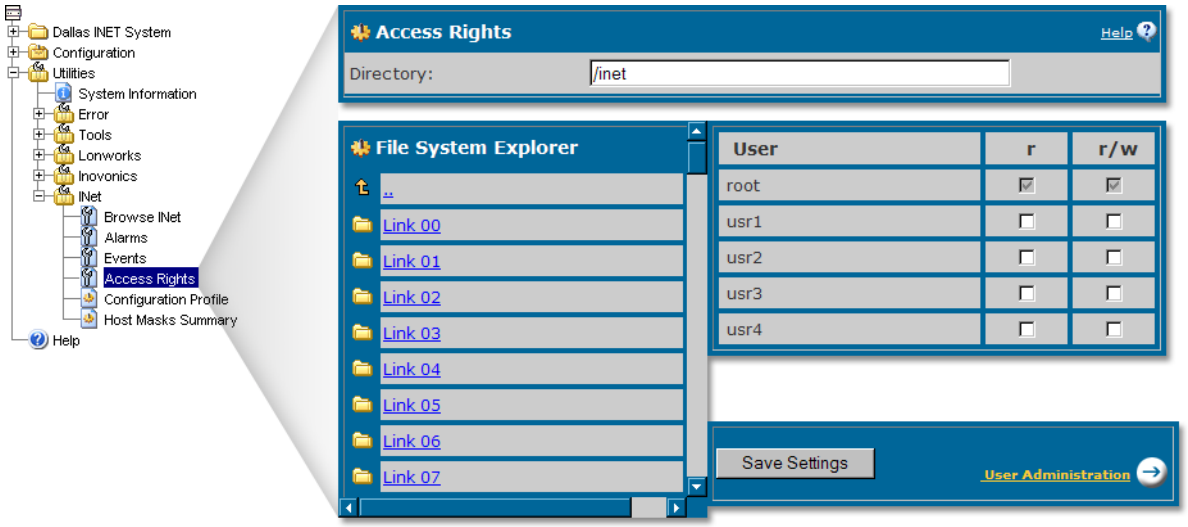


Fig. 5.3: Assigning User Access Rights to I/NET Links

After you penetrate a link, the stations available for that link are displayed. You can continue assigning user access rights as necessary to each station.

Ultimately, a user's access rights will be determined by the combination of their link access rights, station access rights, and user authority.

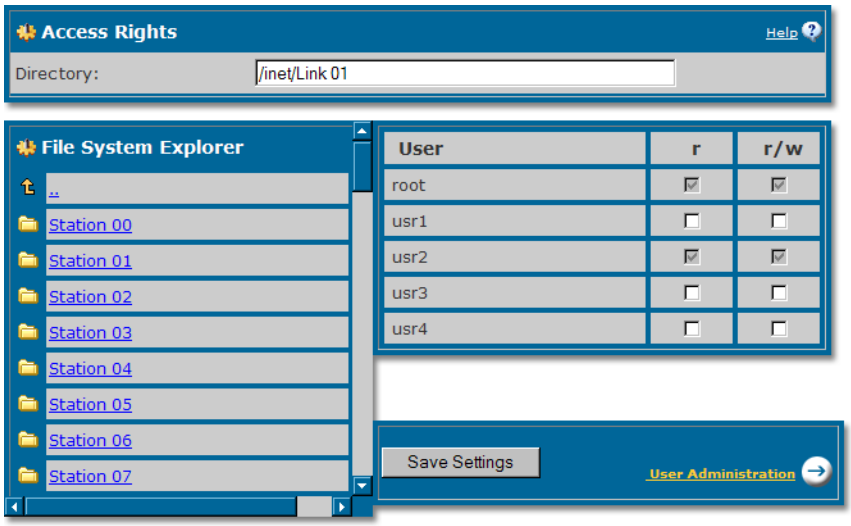


Fig. 5.4: Assigning User Access Rights to I/NET Controllers

The available selections are:

Link 00 Station 00
Station 01
Station 02
..
Station 63

Link 01 Station 00
Station 01
Station 02
..
Station 63

..

Link 99 Station 00
Station 01
Station 02
..
Station 63

The four first characters of the User name are used as a signature in connection with events and alarms.

I/NET User access rights are stored in a system file. This file can only be edited in the system using the web browser, although the file may be stored in the corresponding XBuilder project.

5.3 Logging Failed Login Attempts

The system creates a log file of any failed log in attempts. The log file keeps the latest 50 entries. Each entry is 176 bytes. You can view the log file by selecting **Utilities ▸ Error ▸ Login Error Log** in the System view.

The errors shown are registered in the system login error log. The format is as follows:

host - user date “url + error text” http status 0

Example:

172.20.10.105 - 203-008-01 01/Jun/2001:08:22:26 +0000 "GET /www/index/index.html HTTP/1.1

Error: Bad Portal timestamp TS=20010404120000" 403 0

Here is a brief description of the error components:

Heading	Description
host	The fully qualified domain name or IP address of the connecting machine.
user	The user ID used in the request.
date	Date and time when error occurred.
“url + error text”	The http method and URL. An error explanation is added.
http status	The http error code.

5.4 Extending Time Between Failed Login Attempts

As a deterrent to unauthorized users, the system takes an increasing amount of time between log in attempts upon each failure. A login delay is introduced separately, based on the user’s User ID and IP address, as follows:

- After 3 consecutive login failures, the login is disabled for 1 minute.
- After the next login failure, the login is disabled for 2 minutes.
- After the next login failure, the login is disabled for 3 minutes.
- After the next login failure, the login is disabled for 4 minutes.
- After the next and following login failures, the login is disabled for 5 minutes.

A successful login or a system restart (RELOAD, WARMSTART, COLDSTART) will reset the login attempt delay.

5.5 Configuring Secure Socket Layer Connections

SSL is short for Secure Sockets Layer, a protocol developed by Netscape for transmitting private documents via the Internet.

SSL works by using a public key to encrypt data that is transferred via the SSL connection. Both Netscape Navigator and Internet Explorer support SSL, and many web sites use the protocol to obtain confidential user information, such as credit card numbers.

SSL uses certificate-based authentication.

The TAC Xenta 527 is, by default, configured with a self-signed certificate from the factory. Some web browsers require parameters in the certificate to be set according to the web site name, i.e. the IP address or a DNS name. The SSL certificate generator creates a new certificate with the correct parameter settings.

Certificates are used for the authentication and secure exchange of information on non-secured networks, such as the Internet. Most commonly, server certificates are used to enable clients to verify the authenticity of web sites.

Two Different Certificates, Self-Signed and CA

In XBuilder you can choose between two types of certificates, self-signed certificates and CA certificates.

Self-Signed Certificates

Self-Signed Certificates are created locally and thus not installed in your browser. When a Self-Signed Certificate is used, the certificate must also be installed on the client i.e. the computer used to browse the Xenta 527.

The Xenta 527 device must be restarted to enable the new certificate. The new certificate is accepted by browsers and may be installed.

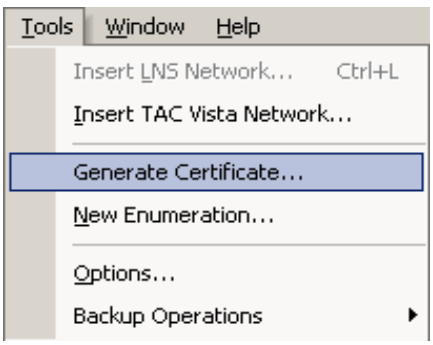
The Getting Started section of this manual explains how to create and use a self-signed certificate.

CA Certificates

CA Certificates are issued by trusted certificate authorities (CAs) like Verisign. These certificates are already installed with the Internet browser. Thus, when using a CA Certificate, there is no need to do anything to the client i.e. the computer used for browsing the Xenta 527.

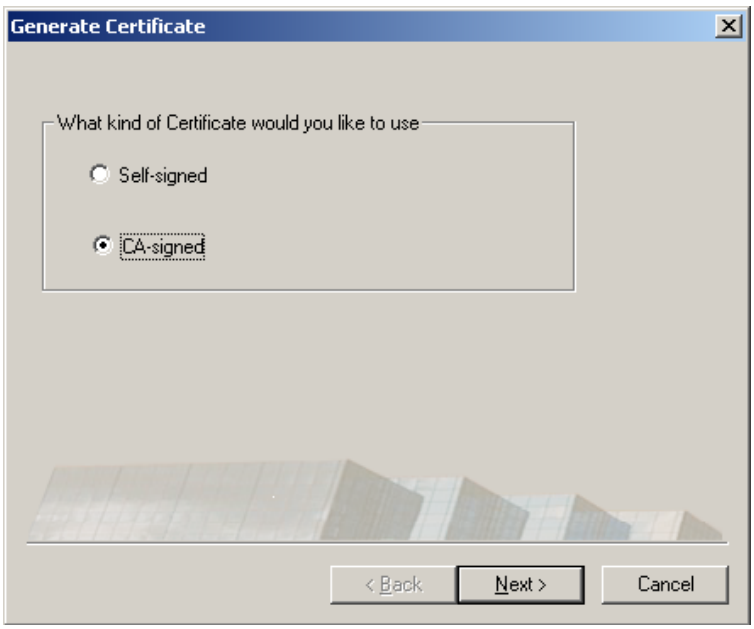
Using a CA Certificate

1 Within an opened project in XBuilder, select **Tools ▸ Generate Certificate** from the menu.

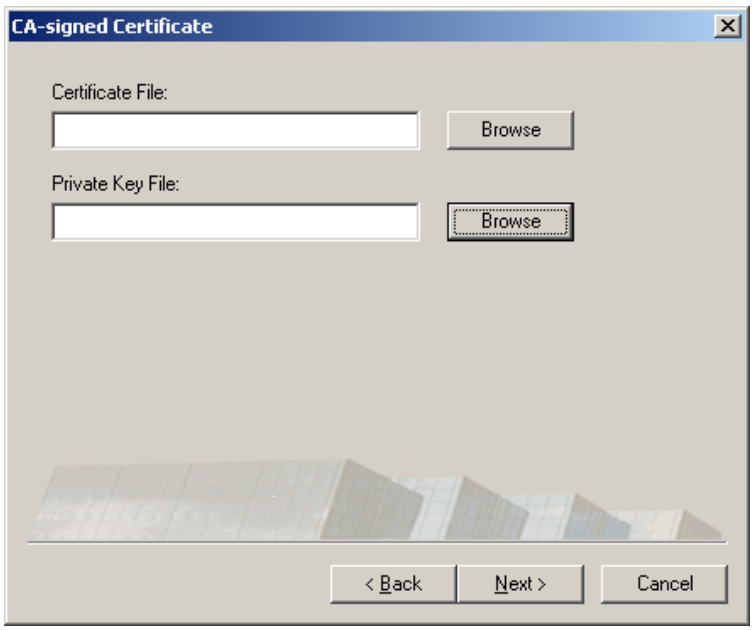


The **Generate Certificate** dialog opens.

2 Use the radio button and select **CA-signed**. Click **Next**.

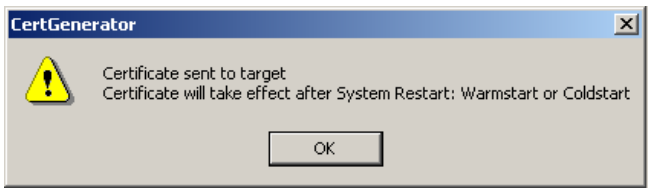


3 Use the **CA-signed Certificate** dialog to browse to the certificate and the private key.



4 Click **Next** and then **Finish** to send the certificate to target.

5 The Xenta 527 has to be restarted for the certificate to take effect.



Note that the CA Certificates are already installed with the browser. Thus, nothing has to be done to the client computer, (i.e. the computer containing the browser that is used to connect to the TAC Xenta 527.)

5.6 Preventing Remote Configuration Clients from Altering Parameters

Local commands to prevent or allow remote configuration can be issued to the Xenta 527 from a console window. This will require that you connect a serial cable between the Xenta 527 and your PC workstation. You can then use a terminal emulator such as Windows Hyperterminal to communicate with the Xenta 527. If necessary, refer to Fig. 2.1 (*page 15*) to view a typical serial cable connection.

By default, remote configuration is enabled. Regardless of the which state is selected (i.e., enabled or disabled), the default state of “enabled” is reinforced following a system restart RELOAD (typically at installation). Other restart types will keep the selected state.

You can *disable* remote configuration by issuing the following command on the local console:

> disrcfg<CR>

This command will *disable* remote configuration of the following parameters:

- DHCP enable/disable
- IP-address
- Subnet mask
- Default gateway
- DNS
- Website name
- Domain name
- Host name
- HTTP port
- HTTPS port
- `Dynamic variables communication Port` issued from the web interface.

You can *enable* remote configuration by issuing the following command on the local console:

>enrcfg<CR>

This command will *enable* remote configuration of the parameters listed above.

6 Creating Web Pages with XBuilder

6.1 Using XBuilder

When you create an XBuilder project that uses the Xenta 527 template, an "INET" object becomes available (see the figure below). This object provides functions that allow you to add I/NET-related items to your project.

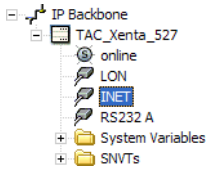


Fig. 6.1: The INET Object in XBuilder

The DCU-to-XML Conversion Tool

The "INET" object in XBuilder relies on an DCU-to-XML conversion tool that is included in the XBuilder installation. This tool converts I/NET SAV files into an XML file that can then be imported into your XBuilder project. When you import the XML file, XBuilder creates a representation of the I/NET network. Any portions of the I/NET network that are defined in the I/NET SAV files will be included in the associated XBuilder representation.

The I/NET Network in XBuilder

The following figure shows a portion of an I/NET network that has been converted from a SAV file and imported into XBuilder. The figure is annotated to describe how each object in the network view represents a portion of the I/NET network.

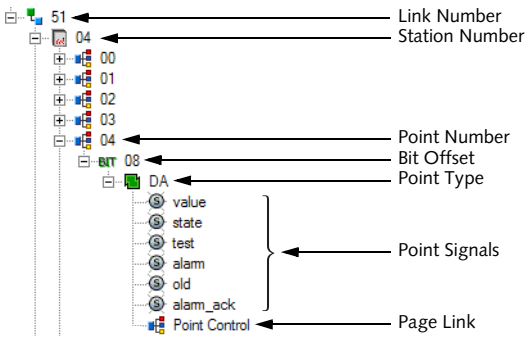


Fig. 6.2: I/NET Point Structure in XBuilder

Sequence of Tasks

The overall sequence that allows you to include I/NET-related items in your project is as follows:

1 Create an XBuilder project that uses the Xenta 527 template.

2 Convert one or more I/NET SAV files to an XML file.

3 Import the XML file in order to create an XBuilder representation of the I/NET network within your project.

4 Add resulting I/NET items to the web pages you create within your project.

6.2 Creating a Project That Will Include I/NET Items

Use the following steps to create an XBuilder project that will contain I/NET-related items.

1 Within XBuilder, start a new project by selecting **File ▸ New Project...** from the main menu.

2 In the Create New Project dialog, perform the following tasks:

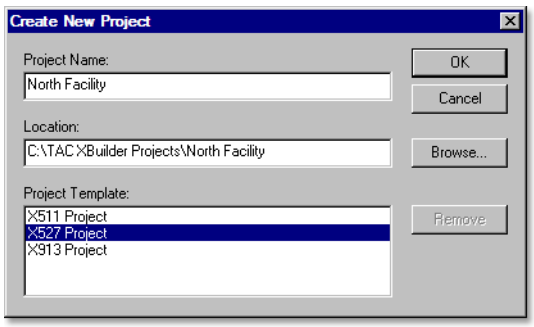


Fig. 6.3: Entering Basic Project Information

a Define a name for the new project.

b Choose the appropriate storage location for the project files.

c Select the **X527 Project** template.

d Select **OK** to save these settings.

3 In the Project Settings dialog, enter a description of the project and set the other parameters as necessary. Select **OK** to continue.

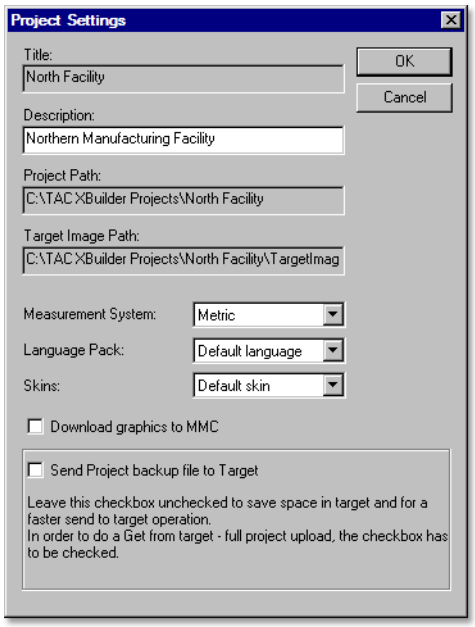


Fig. 6.4: Entering Project Settings

4 In the Network pane of XBuilder, expand the IP Backbone item and verify that an INET object is available.

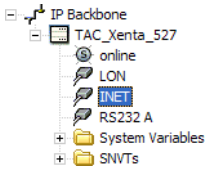


Fig. 6.5: The INET Object in XBuilder

5 Highlight the **INET** object and define IP addresses for up to eight reference hosts. Leave unused addresses set to 0.0.0.0.

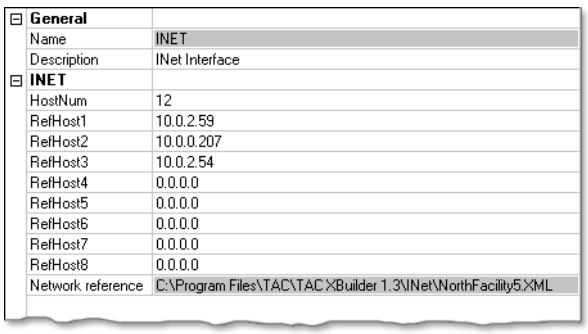


Fig. 6.6: Setting IP Addresses from XBuilder

6 Set the **HostNum** parameter to a value from 1 to 63. This parameter defines the host address that I/NET will use in order to communicate with the Xenta 527. Make sure that the address you define is

unique (i.e., it is not already being used by any other host device on the I/NET network).

6.3 Converting and Importing I/NET SAV Files

Use the following steps to create a representation of the I/NET network within your XBuilder project:

1 Right-click on the INET object and select **Create Network from SAV files** from the resulting pop-up menu.

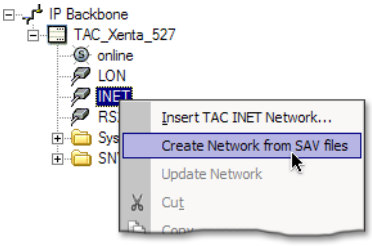


Fig. 6.7: Converting I/NET SAV Files

Note

The utility that converts I/NET SAV files to XML can also be used from outside of XBuilder. Refer to “DCU-to-XML Conversion Utility” on page 61 for more information.

2 In the DCU to XML Conversion dialog, setup the conversion process by completing the following tasks:

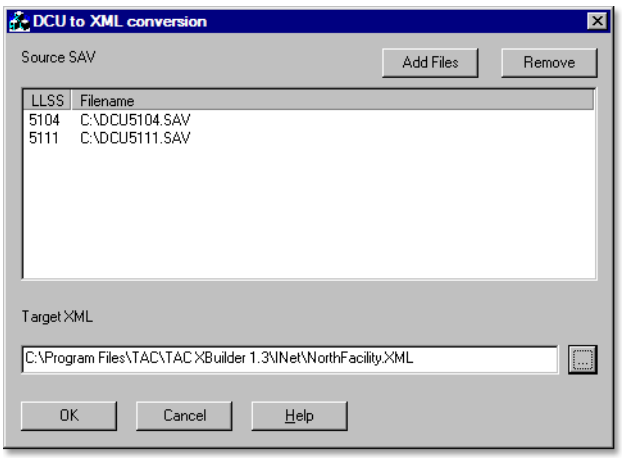


Fig. 6.8: DCU to XML Conversion Dialog

a Use the **Add Files** button to locate and select the I/NET SAV files that you wish to convert. The files you select will appear in the dialog’s Source SAV list.

b Define a complete path and filename for the XML file that the conversion process will create. The **...** button opens a Save As

dialog that you can use in order to browse through your file system.

c Select **OK** to convert the selected SAV files into a single XML file.

3 Import the newly-created XML file by right-clicking the INET object and selecting **Insert TAC INET Network...** from the resulting pop-up menu.

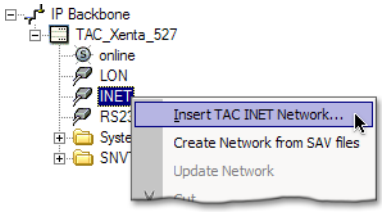


Fig. 6.9: Importing the XML File

4 Select the appropriate XML file and click **Open** to import the file.

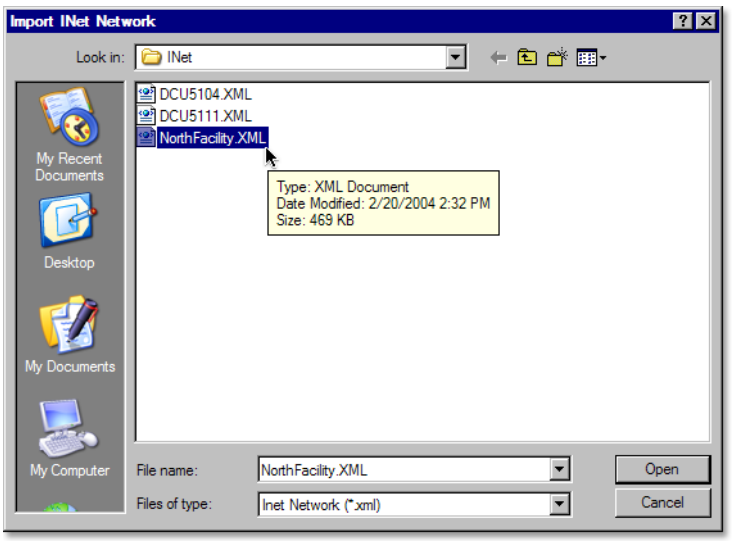


Fig. 6.10: Selecting the XML File

5 Expand the INET object and verify that your project now contains imported I/NET network objects.

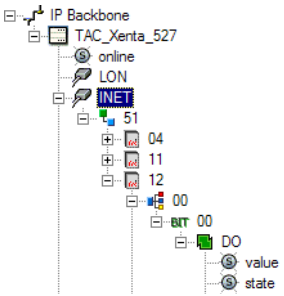


Fig. 6.11: Viewing the Imported I/NET Network

6.4 Updating Your Project with New I/NET SAV Files

Modifications within your I/NET system such as adding or deleting points and point extensions will cause SAV files to change. If changes occur in any of the I/NET SAV files that you have already converted and imported into your project, you must update your project so that it accurately represents the modified I/NET network. This will require that you convert updated I/NET SAV files to a new version of the XML file that you imported earlier.

Use the following steps to update the network in your project:

1 Right-click on the INET object and select **Create Network from SAV files** from the resulting pop-up menu.

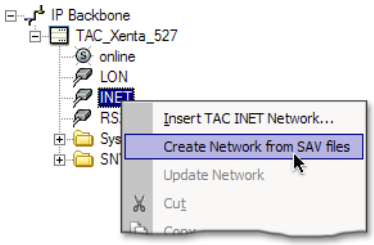


Fig. 6.12: Converting I/NET SAV Files

2 In the DCU to XML Conversion dialog, setup the conversion process by completing the following tasks:

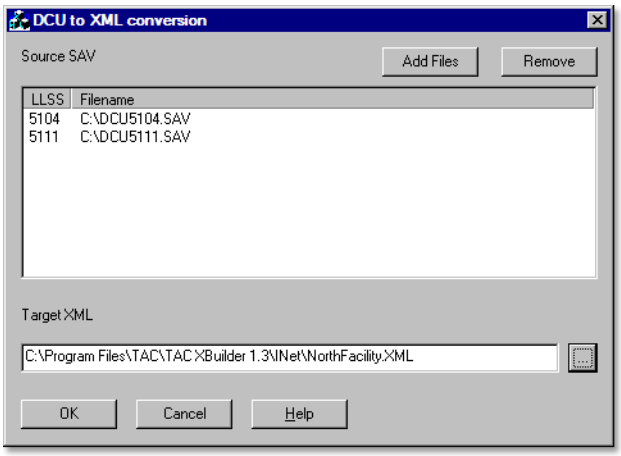


Fig. 6.13: DCU to XML Conversion Dialog

a Use the **Add Files** button to locate and select the updated I/NET SAV files that you wish to convert. The files you select will appear in the dialog's Source SAV list.

b Define a complete path and filename for the XML file that the conversion process will create. Be sure to specify the same path and filename for the resulting XML file that you defined earlier, when you built the network in your current project.

c Select **OK** to convert the selected SAV files into a single XML file.

3 Update the network in the project by right-clicking the INET object and selecting **Update Network** from the resulting pop-up menu.

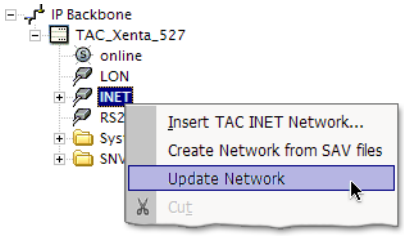


Fig. 6.14: Updating the Network

XBuilder automatically selects the same XML file that was last imported, and then re-imports it.

4 Expand the INET object and verify that your project now contains updated I/NET network objects.

6.5 Displaying Dynamic I/NET Alarms and Events from Web Pages

Note

Alarm and Event pages use Java to display dynamic information. If a user attempts to view these pages from a web browser that is not Java-enabled, no data will display.

In the following example, we will configure the project to provide Java-enabled I/NET alarms and events pages.

1 Add an alarm page to the project by right-clicking the site in the system view and selecting **Add Page ▸ Alarm Page** from the resulting pop-up menu.

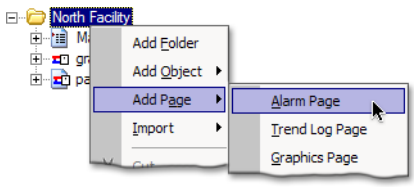


Fig. 6.15: Adding an Alarm Page

2 Type a name for the new alarm page. In this example, we will name the page "North Facility Alarms".

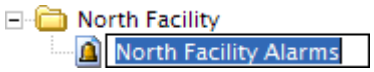


Fig. 6.16: Naming the Alarm Page

3 Make sure that the **Show Dynamic Alarms** parameter is set to "Yes". This setting will allow I/NET alarms to display, rather than Vista alarms.

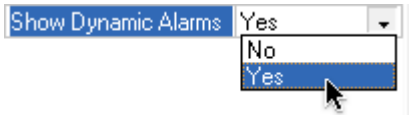


Fig. 6.17: Showing Dynamic Alarms

4 Add an event page to the project by right-clicking the site in the system view and selecting **Add Page ▸ Event Page** from the resulting pop-up menu.

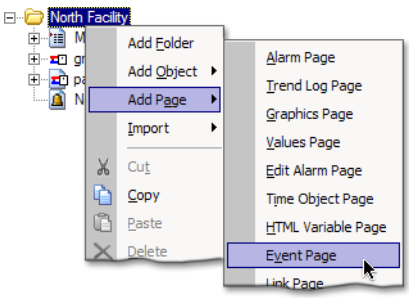


Fig. 6.18: Adding an Event Page

5 Type a name for the new event page. In this example, we will name the page "North Facility Events".

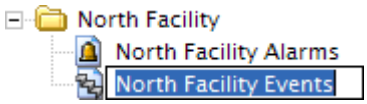


Fig. 6.19: Naming the Event Page

6 By default, the event page will provide I/NET event data. You can confirm this by making sure that the **Event Type** parameter is set to "InetAMT."

Fig. 6.20: Setting the Event Type

7 Highlight the "TAC_Xenta_527" object in the network pane and make sure that the **IP address**, **Username** and **Password** parameters are defined.

Fig. 6.21: Checking the IP Address, Username, and Password

8 Compile the project and send it to the Xenta 527. Using a Web browser, verify that the alarm and event pages display properly.

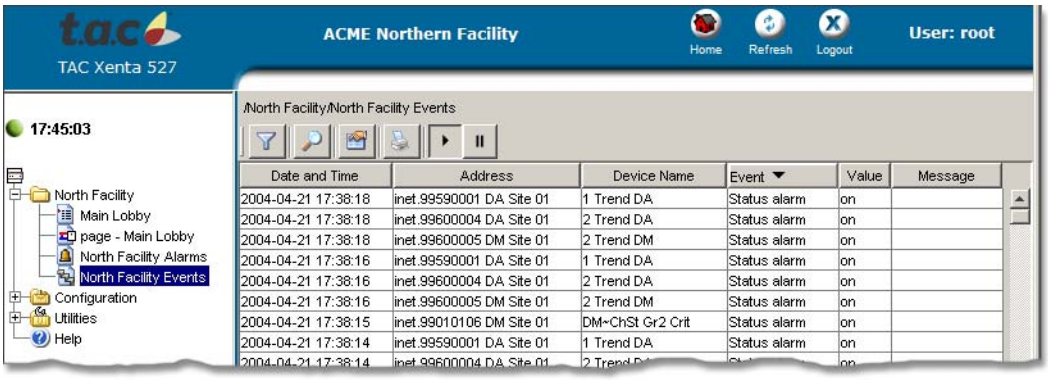


Fig. 6.22: Viewing the Event Page from a Web Browser

6.6 Using I/NET Point Signals

Within XBuilder, each I/NET point has associated signals. A point signal represents one particular aspect of the point. For example, the "value" point signal represents the point's current value. For a description of each I/NET point signal, refer to "Point Signals" on page 68.

You can use I/NET point signals within web pages and graphic pages in your project. The procedures for doing so are described below.

6.6.1 Mapping I/NET Point Signals to Web Pages

Mapping an I/NET point to a web page can be as easy as dragging a signal from XBuilder's network view and dropping it onto the appropriate web page in the system view. The way the point information on a page is displayed to the user, and the way it can be used, depends on the type of web page on which it resides.

In the following example, we will map I/NET point information to a values page.

1 Add a values page to the project by right-clicking the site in the system view and selecting **Add page ▸ Values page** from the resulting pop-up menu.

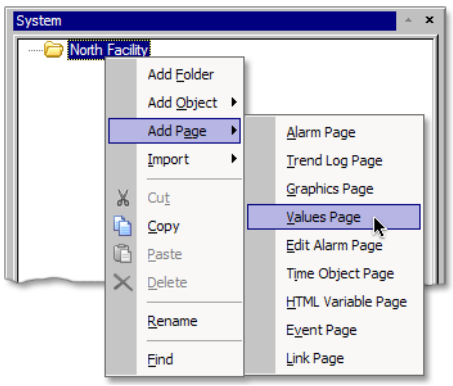


Fig. 6.23: Adding a Values Page

2 Type a name for the new values page. In this example, we will name the page "Main Lobby".

3 Add signals to the values page by dragging signals from the network view and dropping them on the values page. In this example, we will add the value, state, test, alarm, old, and alarm_ack signals for I/NET point 51040408 DA to the values page.

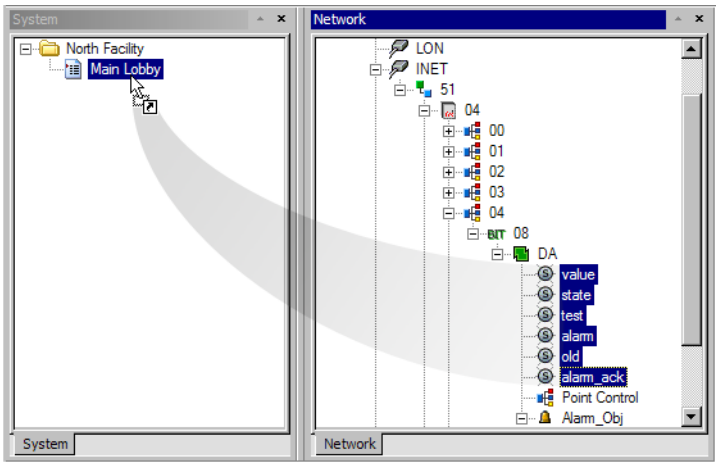


Fig. 6.24: Adding Signals to a Values Page

4 For each signal, enter a description. This text is what will appear on the resulting web page, and should therefore, be useful to the end-user.

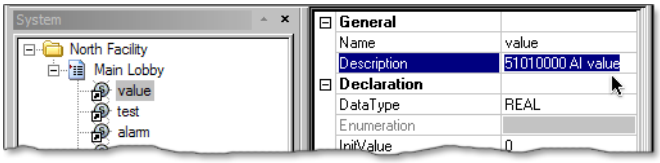


Fig. 6.25: Entering a Description of the Signal

5 Compile the project and send it to the Xenta 527. Using a Web browser, verify that the web page displays properly.

Note

When viewing a point's value, be aware that the Xenta 527 uses an Ansi-C 32-bit standard for floating points. Point values that exceed this limit of floating points are subject to inconsistent displays.

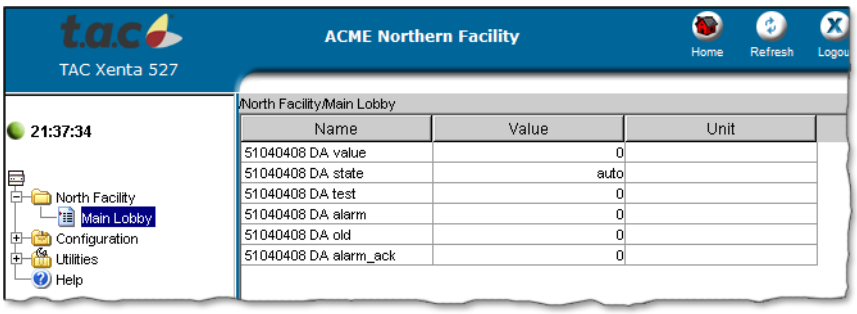


Fig. 6.26: Viewing the Values Page from a Web Browser

6.6.2 Mapping I/NET Point Signals to Graphic Pages

In the following example, we will map I/NET point information to a graphic page.

1 Add a graphic object to the project by right-clicking the site in the system view and selecting **Add Object ▸ Graphic** from the resulting pop-up menu.

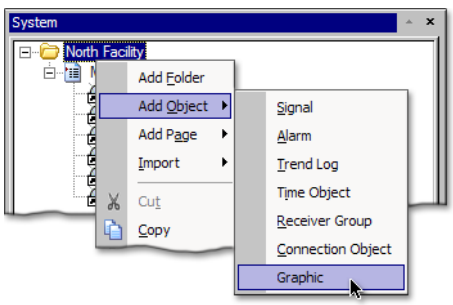


Fig. 6.27: Adding a Graphic Object

2 In the New Graphic dialog, specify a name and location for the new graphic.

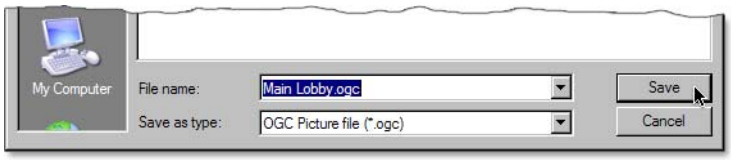


Fig. 6.28: Saving the New Graphic Object

3 Type a name for the new graphic object. In this example, we will name the object "graphic - Main Lobby".

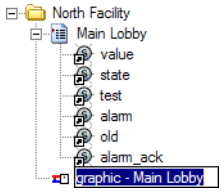


Fig. 6.29: Naming the New Graphic Object

4 Open the new graphic in the Vista Graphic Editor by right-clicking the object and selecting **Edit Graphic...** from the resulting pop-up menu.

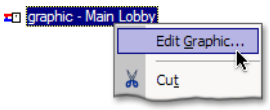


Fig. 6.30: Editing the Graphic

5 Add a new item to the page by clicking a tool in the Drawing Tools toolbar and then clicking on a blank area in the graphic

page. In this example, we will add a Digital Presentation object to the page and assign it an I/NET point value.

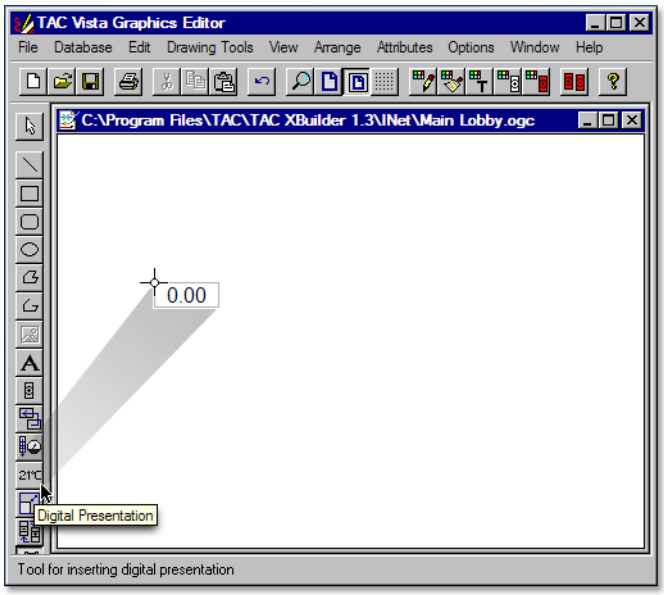


Fig. 6.31: Adding an Object to the Graphic Page

6 Right-click anywhere on the graphic page to change your cursor back into an arrow.

7 Now double-click the new item on the graphic page to view its attributes.

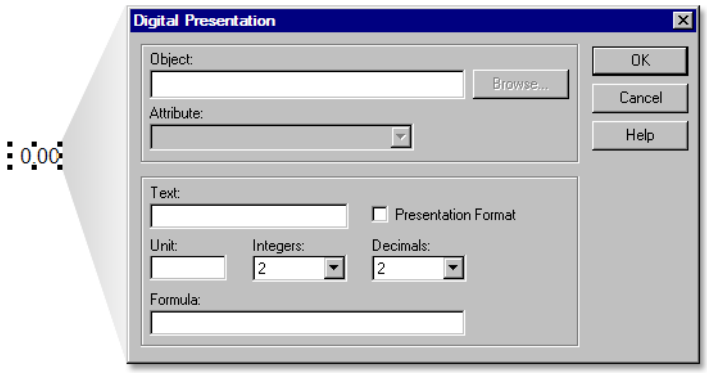


Fig. 6.32: Viewing the Item's Attributes

8 Link an I/NET point value to the graphic object by dragging a "value" signal from XBuilder and dropping it onto the Object field in the attributes dialog.

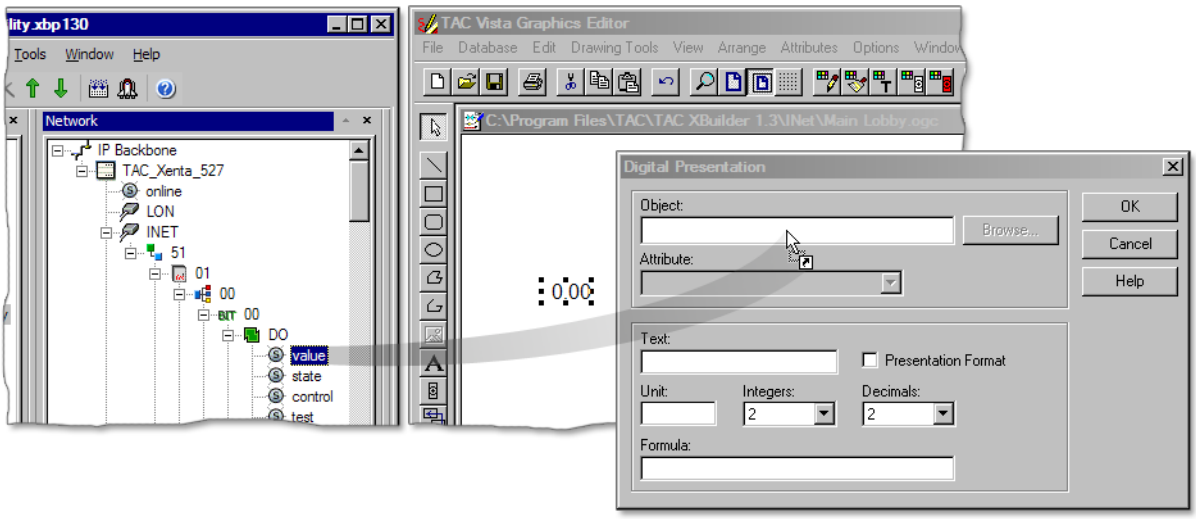


Fig. 6.33: Dragging and Dropping a Signal

9 The **Object** field now contains the path of the signal that you just dropped. Set the other parameters in the attributes dialog as desired and click **OK** to save your settings.

10 Save the graphic and return to XBuilder. Verify that the graphic object in the system view now has a child item representing the signal that you just linked to the graphic.

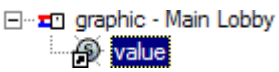


Fig. 6.34: Verifying the Linked Signal

11 Add a graphic page to the project by right-clicking the site in the system view and selecting **Add Page ▸ Graphic Page** from the resulting pop-up menu.

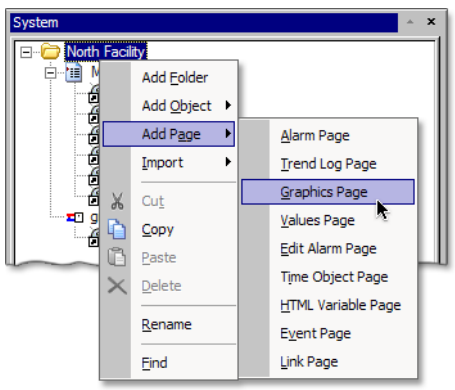


Fig. 6.35: Adding a Graphic Page

12 Type a name for the new graphic page. In this example, we will name the page "page - Main Lobby".

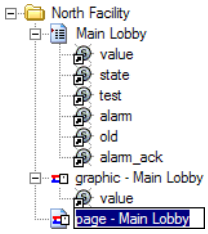


Fig. 6.36: Naming the New Graphic Page

13 Link the graphic object to the graphic page by dragging and dropping the object onto the page.

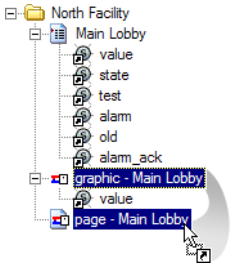


Fig. 6.37: Linking a Graphic Object to a Graphic Page

14 Verify that the graphic page in the system view now has a child item representing the graphic that you just linked to the page.

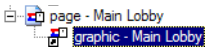


Fig. 6.38: Verifying the Linked Graphic

15 Compile the project and send it to the Xenta 527. Using a Web browser, verify that the graphic page displays properly.

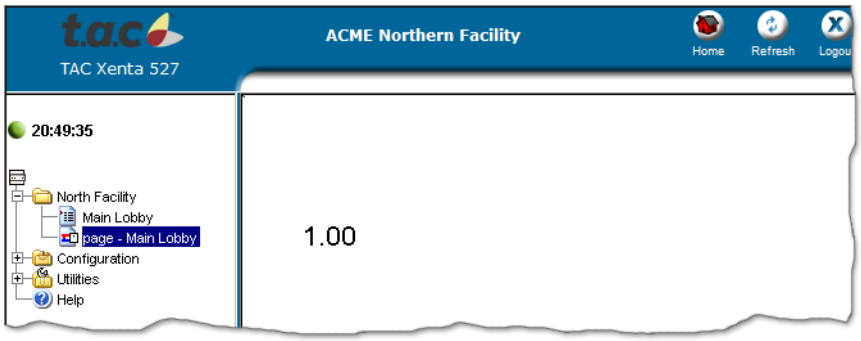


Fig. 6.39: Viewing the Graphic Page from a Web Browser

6.7 Using I/NET Page Links

In addition to the point signals that are associated with an I/NET network in XBuilder, page links are also available. The following I/NET page links can be used within your project and are further described in “Page Links” on page 69:

- **Point Control** – Links to the Point Control page. This page link is included with all I/NET points.
- **Trend** – Links to the Trend Setup page. This page link is included with I/NET points that have a trend (TR) extension.
- **Trendlog** – Links to the Trend Chart page. This page link is included with I/NET points that have a trend (TR) extension.
- **Time Schedule** – Links to the Time Schedule page. This page link is included with I/NET points that have a time schedule (TS) extension.

An I/NET page link can be connected to a standard link page in XBuilder. The link page can optionally be connected to a graphic page, allowing a user to click on a defined area in the graphic to jump directly to the appropriate I/NET page. The procedures for creating these connections are the same for each type of I/NET page link. For your convenience, procedures for linking the Trendlog and Time Schedule pages to a graphic page are described below.

6.7.1 Linking an I/NET Trend Log to a Graphic Page

As a system administrator or user with "operator" privileges, you can access an I/NET trend log by connecting to the Xenta 527 from a web browser, selecting **Utilities ▸ INet ▸ Browse I/NET** from the navigation tree, and browsing the I/NET system. Using this method, you can locate an I/NET point that has a TR (trend) extension, configure the trend log as necessary, and then view the trend log.

A quicker way to access a trend log would be to jump to it from a link, without having to browse through the I/NET system. In the following

example, we will create a link page that links directly to an I/NET trend log, and then associate the link page with a link area on a graphic page.

1 Add a Link Page to the project by right-clicking the site in the system view and selecting **Add Page ▸ Link Page** from the resulting pop-up menu.

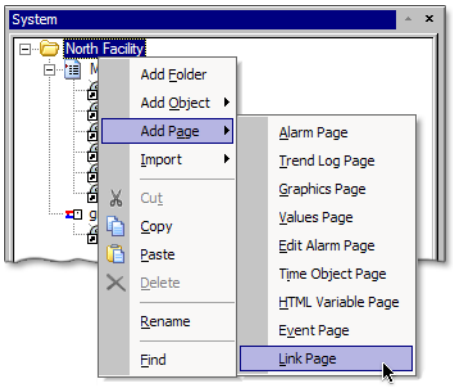


Fig. 6.40: Adding a Link Page

2 Type a name for the new link page. In this example, we will name the page "link - Trend Log".

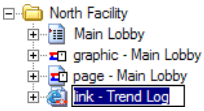


Fig. 6.41: Naming the New Link Page

3 Expand the link page object to expose its link.

Fig. 6.42: Expanding the Link Page Object

4 Associate the link with an I/NET trend log by dragging and dropping a Trendlog object onto the link object.

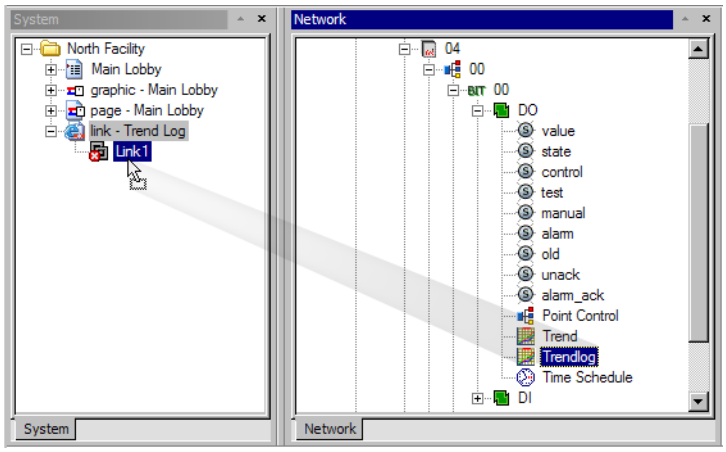


Fig. 6.43: Creating a Link to an I/NET Trend Log

5 Now that you have created a link page that jumps to an I/NET trend log, you can associate the link page with a link area on a graphic page.

Perform one of the following tasks:

- Open an existing graphic object by right-clicking the object and selecting **Edit Graphic...** from the resulting pop-up menu.
- Add a new graphic object to the project by performing the first 4 steps in “Mapping I/NET Point Signals to Web Pages” on page 47.

6 Add a new link area to the page by clicking the Link Area tool in the Drawing Tools toolbar and then drawing a link area in the graphic page. In this example, we will create a link area around an I/NET point value.

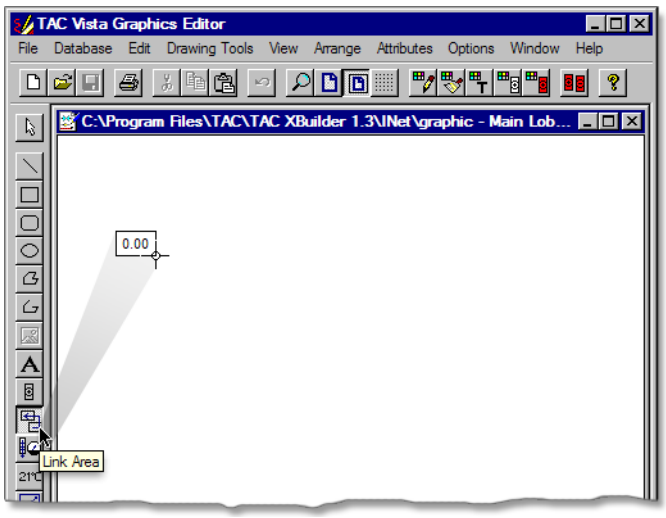


Fig. 6.44: Creating a Link Area on the Graphic Page

7 Right-click anywhere on the graphic page to change your cursor back into an arrow.

8 Right-click the link area and select **Attributes** from the resulting pop-up menu. The Link Area attributes dialog opens.

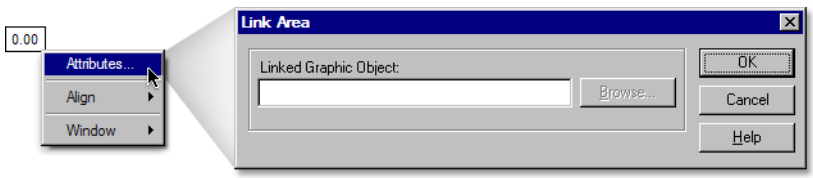


Fig. 6.45: Viewing the Link Area Attributes

9 Associate the link page in XBuilder with the link area on the graphic page by dragging and dropping the link page object onto the **Linked Graphic Object** field in the attributes dialog.

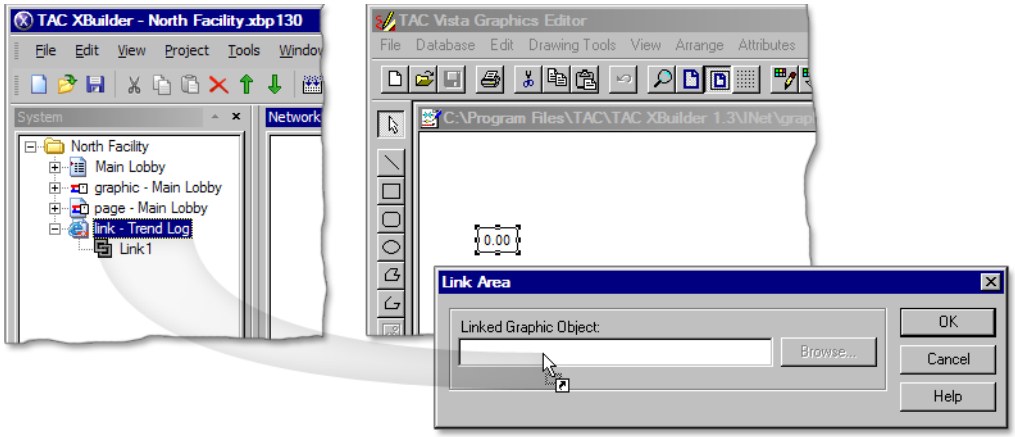


Fig. 6.46: Dragging and Dropping the Link

10 The **Linked Graphic Object** field now contains the path of the link page that you just dropped. Click **OK** to save this setting.

11 Save the graphic and return to XBuilder.

12 Compile the project and send it to the Xenta 527. Using a Web browser, verify that the graphic page now links to an I/NET trend log.

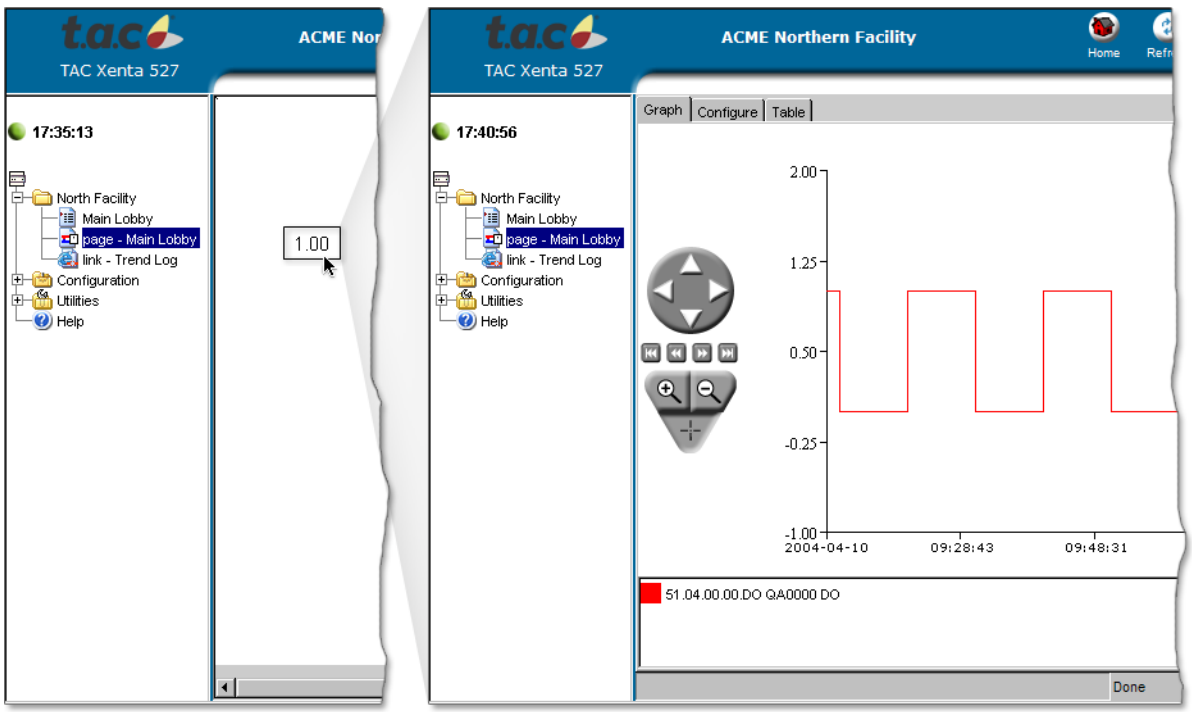


Fig. 6.47: Verifying the Link from a Web Browser

6.7.2 Linking an I/NET Time Schedule to a Graphic Page

The TAC Xenta 527 provides a special editor that allows the system administrator, or a user with "operator" privileges, to modify I/NET Seven time schedules. The user can access this editor by browsing through the I/NET system until they locate an I/NET point that has a TS (time schedule) extension. However, you can also create a link on a graphic page that, when clicked, can send the user directly to a time schedule, without requiring the user to browse through the I/NET system.

In the following example, we will create a link page that connects to an I/NET time schedule, and then associate the link page with a link area on a graphic page.

1 Add a Link Page to the project by right-clicking the site in the system view and selecting **Add Page ▸ Link Page** from the resulting pop-up menu.

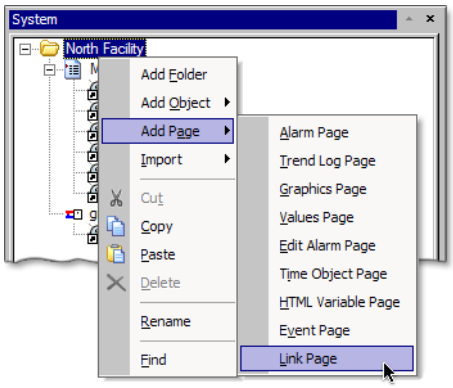


Fig. 6.48: Adding a Link Page

2 Type a name for the new link page. In this example, we will name the page "link - Time Schedule".

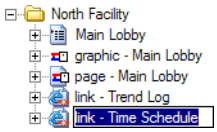


Fig. 6.49: Naming the New Link Page

3 Expand the link page object to expose its link.

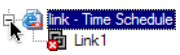


Fig. 6.50: Expanding the Link Page Object

4 Associate the link with an I/NET time schedule by dragging and dropping a Time Schedule object onto the link object.

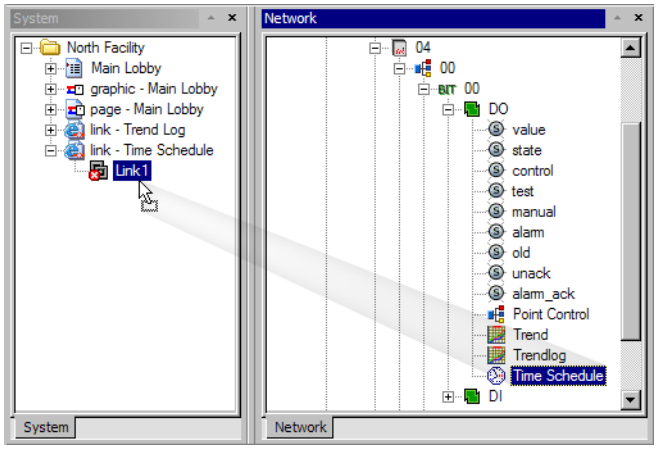


Fig. 6.51: Creating a Link to an I/NET Time Schedule

5 Now that you have created a link page that jumps to an I/NET time schedule, you can associate the link page with a link area on a graphic page.

Perform one of the following tasks:

- Open an existing graphic object by right-clicking the object and selecting **Edit Graphic...** from the resulting pop-up menu.
- Add a new graphic object to the project by performing the first 4 steps in “Mapping I/NET Point Signals to Web Pages” on page 47.

6 Add a new link area to the page by clicking the Link Area tool in the Drawing Tools toolbar and then drawing a link area in the

graphic page. In this example, we will create a link area around a graphic that has been imported into the graphic page.

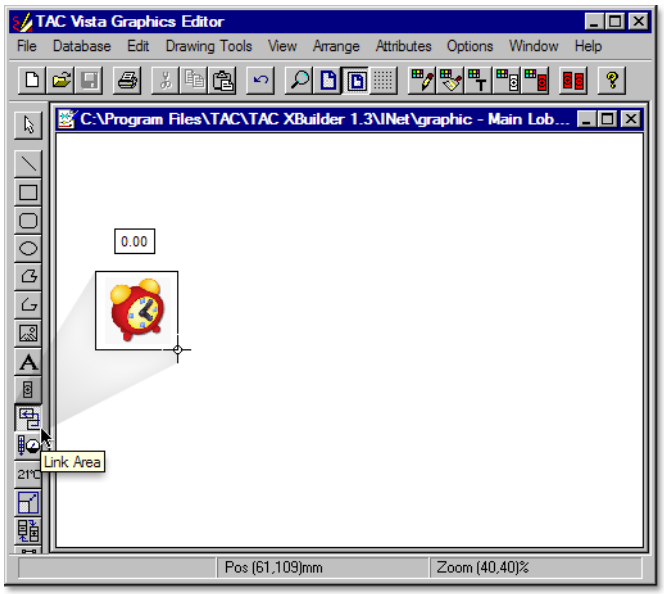


Fig. 6.52: Creating a Link Area on the Graphic Page

7 Right-click anywhere on the graphic page to change your cursor back into an arrow.

8 Right-click the link area and select **Attributes** from the resulting pop-up menu. The Link Area attributes dialog opens.

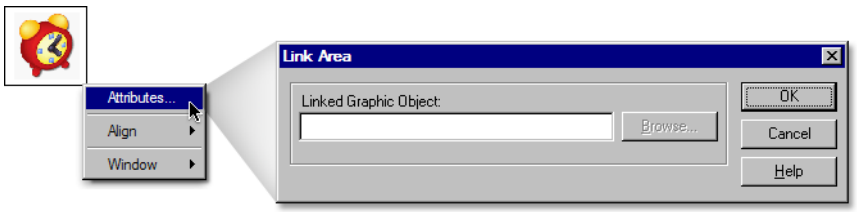


Fig. 6.53: Viewing the Link Area Attributes

9 Associate the link page in XBuilder with the link area on the graphic page by dragging and dropping the link page object onto the **Linked Graphic Object** field in the attributes dialog.

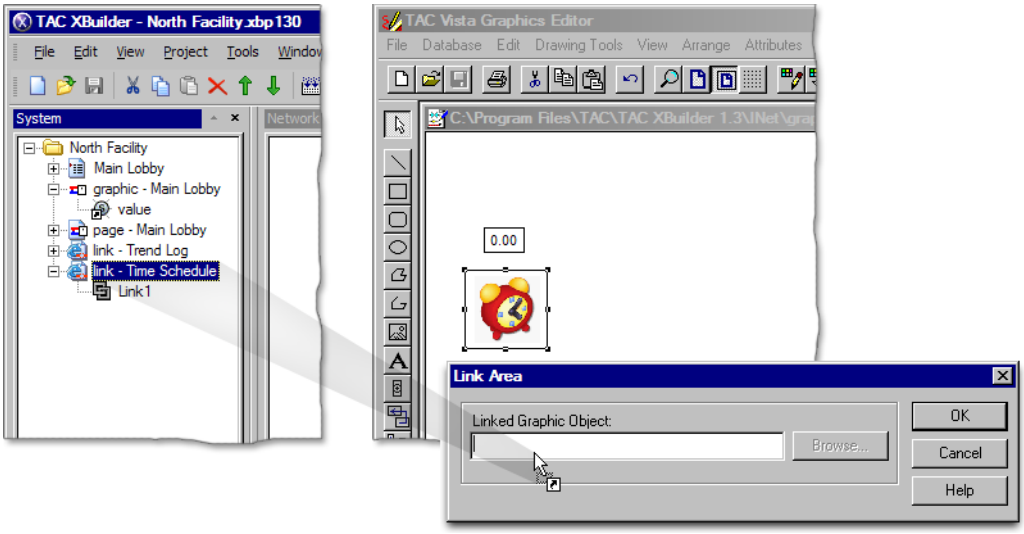


Fig. 6.54: Dragging and Dropping the Link

10 The **Linked Graphic Object** field now contains the path of the link page that you just dropped. Click **OK** to save this setting.

11 Save the graphic and return to XBuilder.

12 Compile the project and send it to the Xenta 527. Using a Web browser, verify that the graphic page now links to an I/NET time schedule.

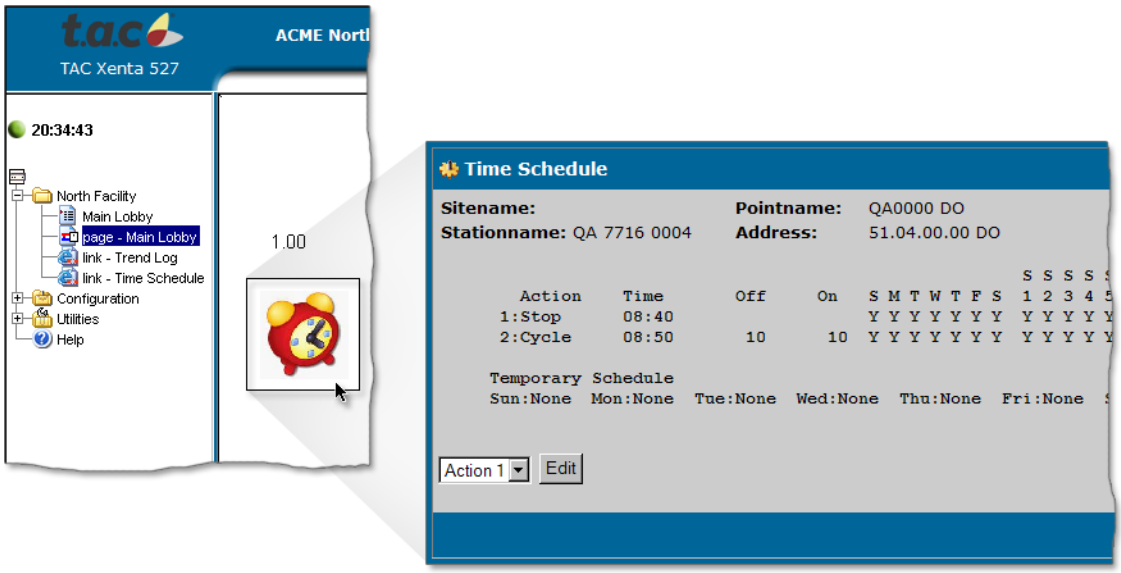


Fig. 6.55: Verifying the Link from a Web Browser

6.8 Using the Find Function

When working on large projects the **Find** function may be used to identify variables and objects in the projects.

1 Activate the find function using any of the following methods:

- Press **Ctrl** + **F**.
- Choose **Edit** ▸ **Find** from the main menu.

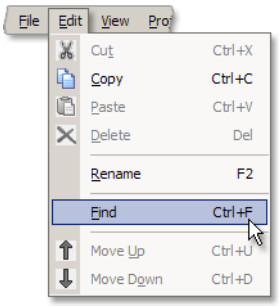


Fig. 6.56: Selecting Find from the Main Menu

- Right-click an item in the System pane or Network pane and select **Find** from the resulting pop-up menu.

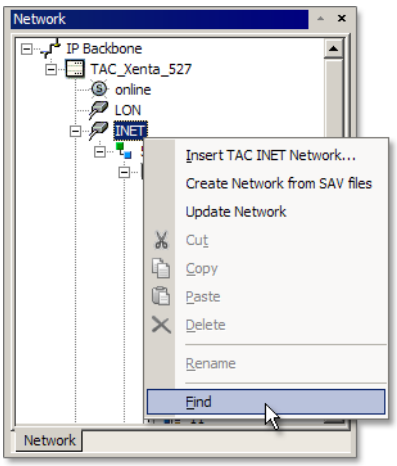


Fig. 6.57: Selecting Find from a Pop-up Menu

2 Use the Find dialog to search through the project. If necessary, narrow the search by specifying which objects, pages, and signals to include in the search. By default, all items are included.

You can also use the **Look in** field to narrow the search to a specific branch of the system or network. This field will automatically con-

tain an appropriate path if you activate the Find function by right-clicking on an item in the System pane or Network pane.

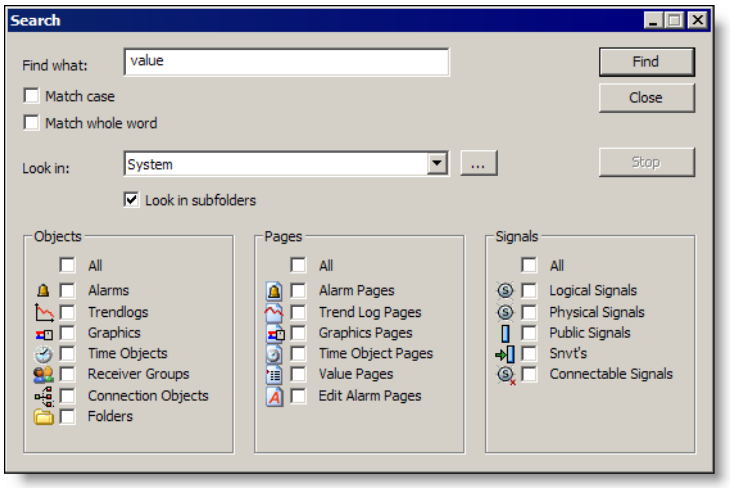


Fig. 6.58: The Find Dialog

3 Click **Find** to begin the search. The results are displayed in the Output pane. A number of options are available when you select an item in the results, as described below.

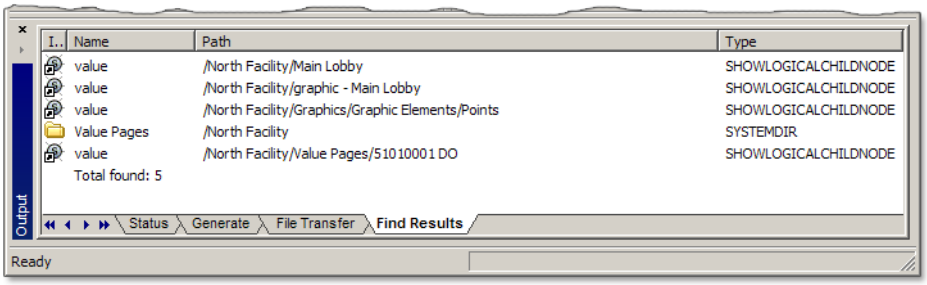


Fig. 6.59: Viewing the Results of the Find Function

- Jump to the source of any item in the results by double-clicking on the item. You can also right-click on the item and select **Go to the source** from the pop-up menu.
- Clear all items by right-clicking on any item in the results and selecting **Clear** from the pop-up menu.
- Delete the source of an item by right-clicking the item in the results and selecting **Delete** from the pop-up menu. The **Delete** option is *not* available for signal objects in the Network pane.
- Rename any item associated with a System pane object by right-clicking the item in the results and selecting **Rename** from the pop-up menu.

REFERENCE

7 I/NET Objects in XBuilder

8 DCU-to-XML Conversion Utility

9 History Logs

10 Storing Data on the Xenta 527

7 I/NET Objects in XBuilder

The following figure shows a portion of an I/NET network in XBuilder. The figure is annotated to describe how each object represents a portion of the I/NET network. Each object is further described below.

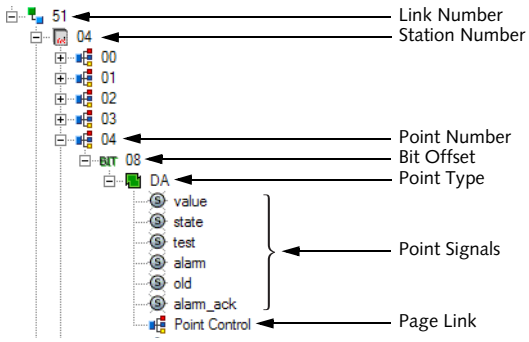


Fig. 7.1: I/NET Point Structure in XBuilder

Each device and point in I/NET has a unique address that identifies it in the system. An address in the I/NET system consists of a series of alpha-numeric characters, each describing the route from the top of the LAN hierarchy to the final device or input/output point. This addressing structure consists of four pairs of numbers and the point type. The format for the address is:

LLSSPPBB PT

where:

LL = the 2-digit link number

SS = the 2-digit station number

PP = the 2-digit point number

BB = the 2-digit bit offset number

PT = the 2-letter point type

These identification numbers are called system addresses. Each point address is determined by the address of the equipment passed through to reach it.

7.1 Network Objects

The following objects in XBuilder represent levels of the I/NET network:

- **Link** — This object represents the software link address (00–99) that leads to a specific I/NET controller LAN. By expanding this object, you can access stations connected to the controller LAN.
- **Station** — This object represents the address (00–63) of a particular controller on the controller LAN. By expanding this object, you can access the points defined for the controller.
- **Point** — This object represents the address (00–31) of a particular memory location within the selected station.
- **Bit Offset** — This object represents the bit offset (00–09) of the the selected memory location.
- **Point Type** — This object represents the two-letter point type designation for the selected point.

7.2 Point Signals

The following I/NET point signals are available in XBuilder. As described below, not all signals are available for all point types.

- **value** (*all point types*) — This signal represents the value of the selected point. For all point types except DC and DO, an operator with proper authority can log into the Xenta 527 and use this signal to view or change the point's value. For DC and DO points, an operator would have to change the value of the "control" signal (described below) in order to change the point's value.
- **state** (*DA, DC, DI, DM, and DO points only*) — This read-only signal shows the textual state of the point. This text is based on the state descriptions assigned to the point in I/NET. Refer to the I/NET Seven documentation for a description of state descriptions.
- **control** (*DC and DO points only*) — Use this signal to manually control the point. This signal's default value is 0. A change in this signal's value causes the value to be sent to the point. Therefore, even if you wish to send the default value of 0 to the point, you must temporarily change the signal's value to 1 and then back to 0. Refer to the I/NET Seven documentation for a description of control descriptions.
- **test** (*all point types*) — This signal represents the value of the point's test mode setting. A value of 1 indicates that the point is operating in test mode. An operator with proper authority can log into the Xenta 527 and use this signal to view or change the point's test mode condition.

- **manual** (*output points only*) — This signal represents the value of the point's manual mode setting. A value of 1 indicates that the point is operating in manual mode. An operator with proper authority can log into the Xenta 527 and use this signal to view or change the point's manual mode condition.
- **alarm** (*all point types*) — This read-only signal represents the value of the point's "alarm" state. A value of 1 indicates that the point is currently in alarm.
- **old** (*all point types*) — This read-only signal represents the value of the point's "old" state. A value of 1 indicates that the point value is invalid or is no longer communicating.
- **unack** (*all point types*) — This read-only signal represents the value of the point's "unacknowledged" alarm state. A value of 1 indicates that the point's alarm is unacknowledged. If an authorized user acknowledges the alarm, this value will change to 0.
- **alarm_ack** (*all point types*) — This signal allows an authorized operator to acknowledge an alarm associated with the point. The user can acknowledge an alarm by setting this signal's value to 1. Once the Xenta 527 verifies that I/NET has acknowledged the alarm, this signal's value will return to 0.

7.3 Page Links

Along with the signals described above, page links are also available for I/NET points. You can add these links to Link Pages within an XBuilder project. As described below, not all page links are available for all points.

- **Point Control** — The Point Control link is included with all I/NET point types. This link allows the system administrator, or a user with "operator" privileges, to access the Point Control screen.

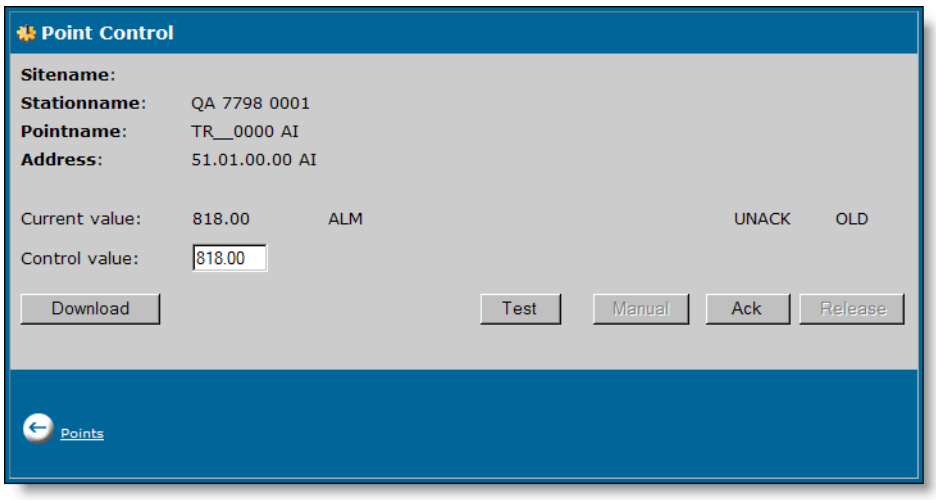


Fig. 7.2: Point Control from a Web Browser

- **Trend** — The Trend link is included with I/NET points that have a Trend Sampling (TR) extension. This link allows the system administrator, or a user with "operator" privileges, to access the Trend Setup screen.

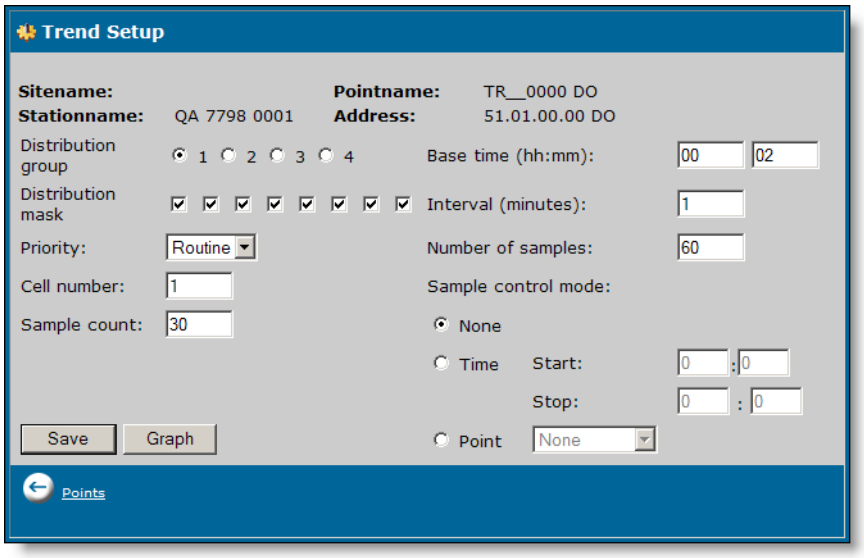


Fig. 7.3: Trend Setup from a Web Browser

- **Trendlog** — The Trendlog link is included with I/NET points that have a Trend Sampling (TR) extension. This link allows the system administrator, or a user with "operator" privileges, to access the Trend chart.

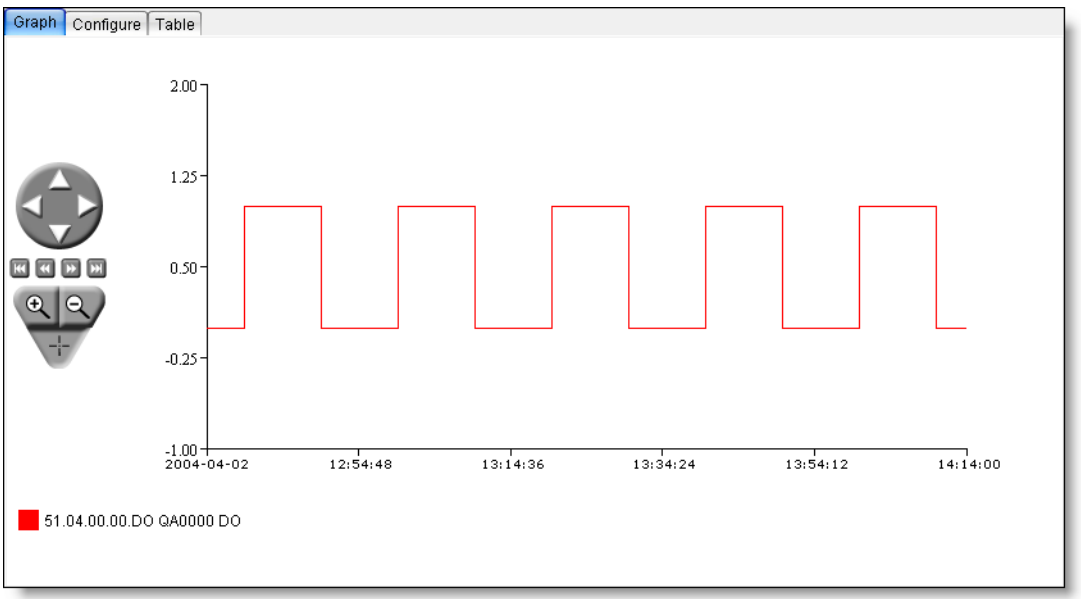


Fig. 7.4: Trend Chart Displayed in a Web Browser

- **Time Schedule** — The Time Schedule link is included with I/NET points that have a Trend Schedule (TS) extension. This link

allows the system administrator, or a user with "operator" privileges, to access the Time Schedule screen.

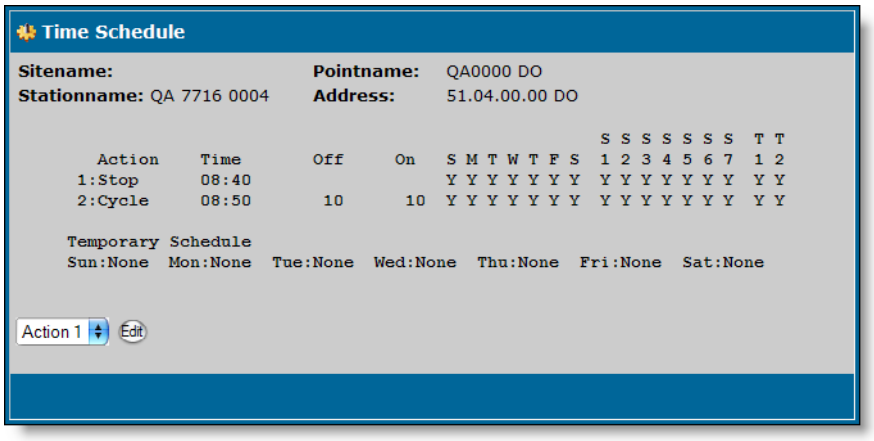


Fig. 7.5: Time Schedule Editor Displayed in a Web Browser

8 DCU-to-XML Conversion Utility

In order to create and use I/NET system objects within XBuilder, you must first convert I/NET SAV files into an XML file that you can then import into your project. This conversion process relies on an I/NET-to-XBuilder utility that is included in the XBuilder installation.

As described in "Converting and Importing I/NET SAV Files" on page 42, you can launch this utility from within XBuilder by right-clicking on the INET object in your project and selecting **Create Network from SAV files** from the resulting pop-up menu. However, you can also launch and use this utility from outside of XBuilder, as described below.

8.1 Launching the Utility from an Explorer Window

The DCU-to-XML conversion utility is located in the XBuilder installation directory. You can launch the utility as a stand-alone application by locating and executing the file named *DCUXML.EXE*. This causes the DCU to XML Conversion dialog box to appear.

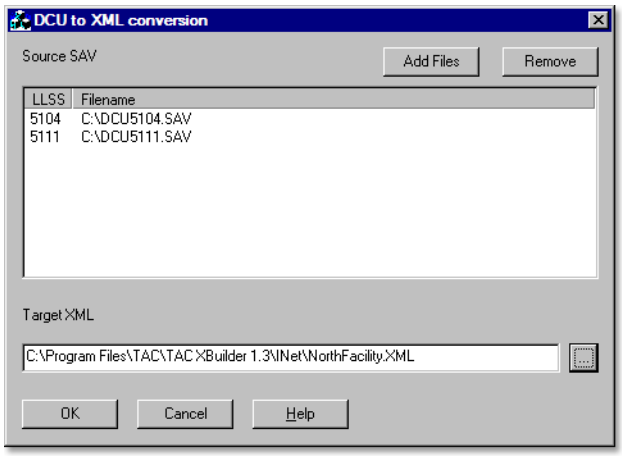


Fig. 8.1: DCU to XML Conversion Dialog

You can use the conversion utility just as if you had launched it from XBuilder. Refer to "Converting and Importing I/NET SAV Files" on page 42 for instructions.

8.2 Running the Utility from the Command Line

The DCU-to-XML conversion utility can be run as a command-line application, as follows:

1 Click the **Start** button in Windows and select **Run...** from the resulting menu. The Run dialog opens.

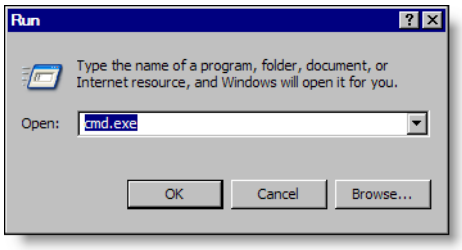


Fig. 8.2: The Run Dialog

2 Type **CMD.EXE** in the text field and select **OK**. A command window opens.

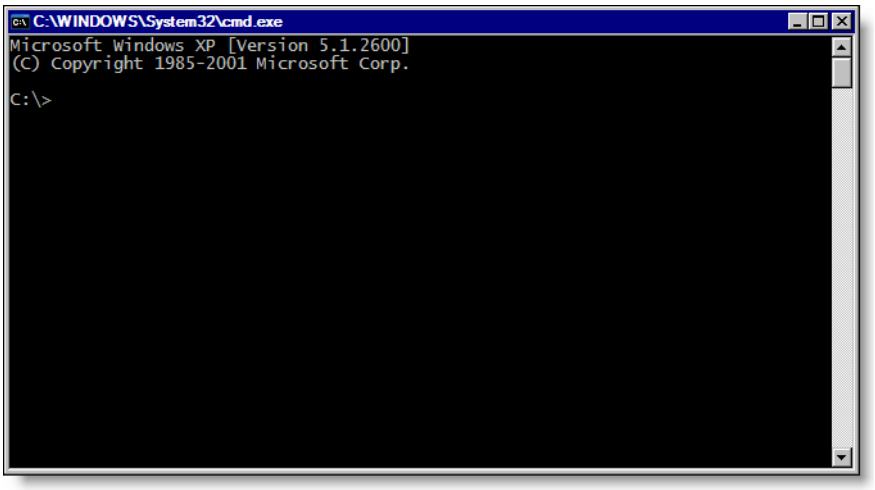


Fig. 8.3: Command Window

3 At the command prompt, use the change directory command (CD) to go to the XBuilder installation directory. In the example below, XBuilder is installed at its default location on C drive.

```
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\>cd C:\Program Files\TAC\TAC XBuilder 1.3.0

C:\Program Files\TAC\TAC XBuilder 1.3.0>
```

Fig. 8.4: Changing to the XBuilder Installation Directory

4 Run the utility using the following syntax:

dcuxml.exe *output_file* *input_file(s)*

Example:

The following command will initiate the conversion of two I/NET SAV files (*DCU5101.SAV* and *DCU5104.SAV*) into an XML output file named *LINK51.XML*. The input files reside in the root directory of C drive (as will the resulting XML output file).

```
dcuxml.exe c:\link51.xml c:\dcu5101.sav
c:\dcu5104.sav
```

Using the command in the example above will cause the utility to open and look like this:

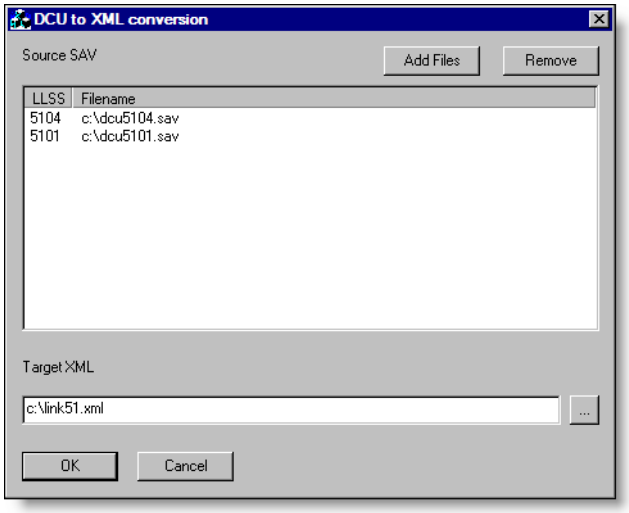


Fig. 8.5: DCU-to-XML Conversion Utility

5 If necessary, make adjustments to the configuration. When the configuration is correct, click **OK** to run the conversion.

6 When the conversion is complete, the utility automatically closes.

9 History Logs

9.1 Occurrences of I/NET System and Web Server Alarms and Events

The TAC Xenta 527 can store a total of 1,000 events and alarms (added together). They are stored in a non-volatile managed memory buffer. This allows the Xenta 527 to maintain its stored events and alarms even during power interruptions.

9.2 Records of Individuals Who Modified an Alarm Status

All changes made to the status of I/NET alarms made by the logged-in user are stored as events in the Xenta 527 memory buffer. These changes are also stored in the I/NET system, and identify the user. The information used to identify the user will differ, depending on how the user made the changes.

I/NET records identify the user as follows:

- When changes are made from the Xenta 527 alarm view, I/NET records will contain the user's initials (i.e., the first 4 characters of the user name) and the user's complete user name.
- When changes are made from a Point Control dialog, I/NET records will contain only the user's initials (i.e., the first 4 characters of the user name).

10 Storing Data on the Xenta 527

10.1 Data Limits

The TAC Xenta 527 has the following data storage limits:

- Max project size = 10 MB
- Max number of Xenta 511 type Alarms = 300
- Max number of Xenta 511 type Trendlogs = 150
- Max number of Xenta 511 type Time Schedules = 50

10.2 Web Server Data

The following Web server data is stored in the TAC Xenta 527:

- User information
  - User information for up to 64 users
  - Client information including passwords and connection information
- Log files containing historical data
- Graphics

10.3 Protecting Stored Data

10.3.1 Maintaining Data During Power Interruptions

The TAC Xenta 527 configuration (including user information and project files) and dynamic data (including alarms, events, and trend logs) is stored in non-volatile memory. This allows the Xenta 527 to maintain its stored information even during power interruptions.

10.3.2 Backing Up and Restoring Data

XBuilder provides the tools necessary to allow you to backup and restore Xenta 527 data files. The following data can be backed up and restored:

- Event Data
- Trend Logs

- Alarm History
- Project Data

Backing Up and Restoring Event, Trendlog, and Alarm History Data

When you backup data from the Xenta 527, the data gets stored with the currently open XBuilder project. If desired, you can then backup the project to further protect the stored data.

The following steps describe how to backup and restore event, trendlog, and alarm history data. Project backup and restore procedures are described separately.

1 Open the project that will be used as the storage location for the data that you are backing up.

2 Select **Tools ▸ Backup Operations** from the XBuilder menu. A sub-menu opens, allowing you to choose the desired operation.

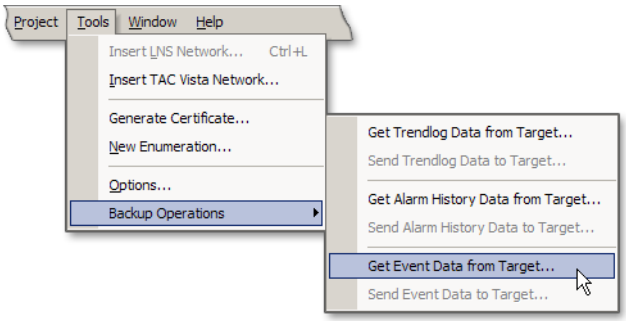


Fig. 10.1: Initiating the Event Data Backup Process

3 Choose the desired operation to backup or restore the associated data.

Backing Up Project Data

Use the following procedures to backup project data:

1 Open the project that you want to back up and view the project settings by selecting **Project ▸ Settings...** from the XBuilder menu.

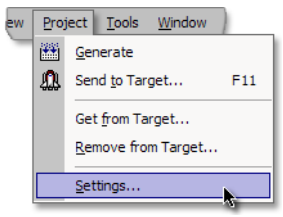


Fig. 10.2: Opening the Project Settings

2 In the resulting dialog box, make sure that the **Send Project backup file to Target** option is activated (☑).

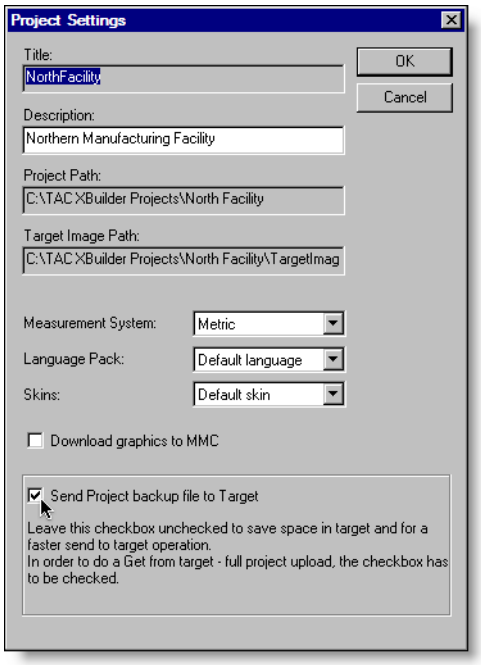


Fig. 10.3: Project Settings

3 Compile the project and send it to the Xenta 527. A backup file will be included in the sent data.

Restoring Project Data

Use the following procedures to restore project data:

1 Restore a project by selecting **Project ▸ Get from Target...** from the XBuilder menu.

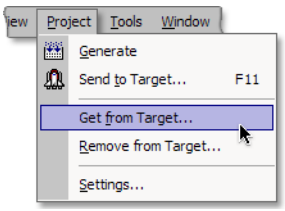


Fig. 10.4: Restoring a Project

2 In the resulting dialog box, specify an appropriate setting for each parameter. If you have a project already open, the fields in this dia-

log will initially contain settings based on the open project. If no project is currently open, the fields will be blank.

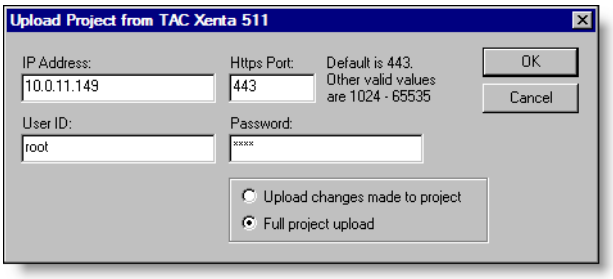


Fig. 10.5: Uploading a Project from the Xenta 527

3 Select **OK** to get the project from the Xenta 527.

4 If differences are found between the currently open project and the project being retrieved from the Xenta 527, they will be displayed in a dialog box. In this case, you can choose which configuration to use. Select either **Project** or **Target**.

Appendix

A Frequently Asked Questions (FAQs)

B Troubleshooting

A Frequently Asked Questions (FAQs)

What if I need to remove the Xenta 527 from the network?

Before you remove the TAC Xenta 527 from the network, you should first remove all host masks that you have defined. This will ensure that other I/NET hosts stop their transmission of alarms and events to the Xenta 527.

Remove host masks as follows:

1 Expand the INet section of the navigation tree as shown in the following figure and select **Host Masks Summary**.

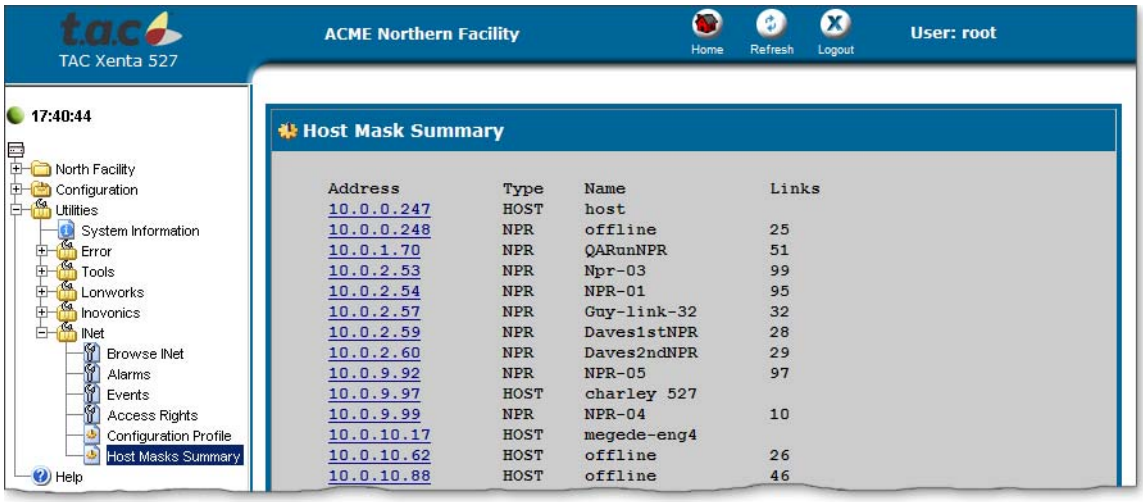


Fig. A.1: Opening the Host Mask Summary

2 In the Host Mask Summary, click on a host IP address to set its routing masks. The Host Routing Mask Editor opens.

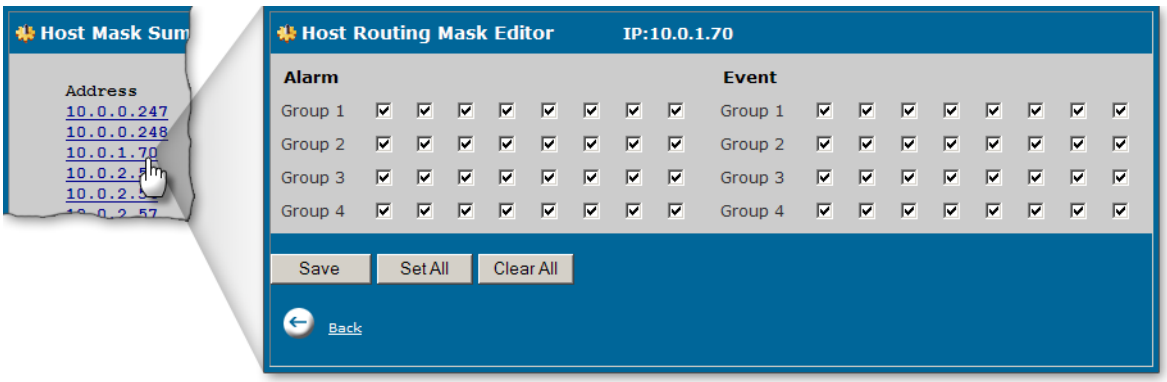


Fig. A.2: Launching the Host Routing Mask Editor

3 Click the **Clear All** button to remove all mask settings for this IP address.

4 Click **Save** to accept your settings.

5 Repeat these steps as necessary to remove the masks for all other IP addresses.

What if I need to perform a full installation of system software for a Xenta 527 that is already operational?

When you load system software onto the Xenta 527, you have a choice of whether to perform a software update or a full installation. If you intend to perform a full installation, you should first remove all host masks that you have defined in the Xenta 527. This will ensure that other I/NET hosts stop their transmission of alarms and events to the Xenta 527.

The steps for the overall process are as follows:

1 Remove all host masks from the Xenta 527. The instructions for removing host masks are described on the previous page.

2 Perform the system software installation as follows:

   a Connect the PC to the same network as the Xenta 527.

   b Start the installation program *TACXenta527-nnnn.exe* (obtained via TARAI or from a CD).

   c Type user name ‘root’, your password, and the TAC Xenta 527’s IP address.

   d Follow the instructions on the screen.

3 When the software installation is complete, re-define host masks on the Xenta 527 as necessary. Refer to “Defining Host Masks”, on page 27 for instructions.

B Troubleshooting

This section addresses common issues that may arise while you are configuring or using the TAC Xenta 527.

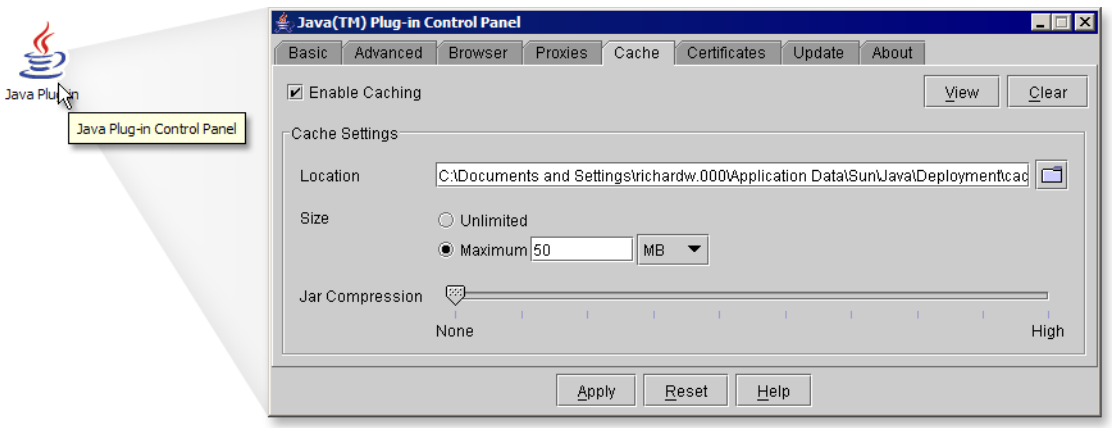
My Alarms and/or Events pages are completely blank

Dynamic alarm and event pages use Java to display periodically updated information. If you attempt to view these pages from a web browser that is not Java-enabled, no data will display.

If Java is properly installed, but alarm and event pages appear blank when you view them from a web browser, you may need to clear the Java cache. The following steps describe how to clear the Java cache:

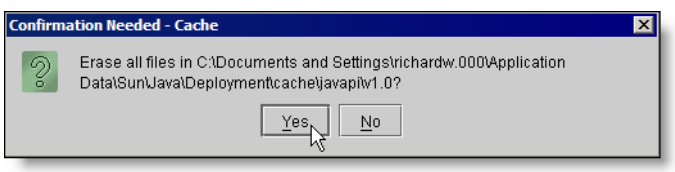
1 Open the Windows Control Panel by clicking the **Start** button and selecting **Control Panel** from the resulting menu.

2 Double-click the Java Plug-in icon to open the Java Plug-in Control Panel. Select the **Cache** panel.



3 Clear the Java cache by clicking the **Clear** button.

4 At the confirmation screen, select **Yes** to clear the cache.



With the Java cache clear, re-connect to the Xenta 527 and verify that alarms and events pages display properly.

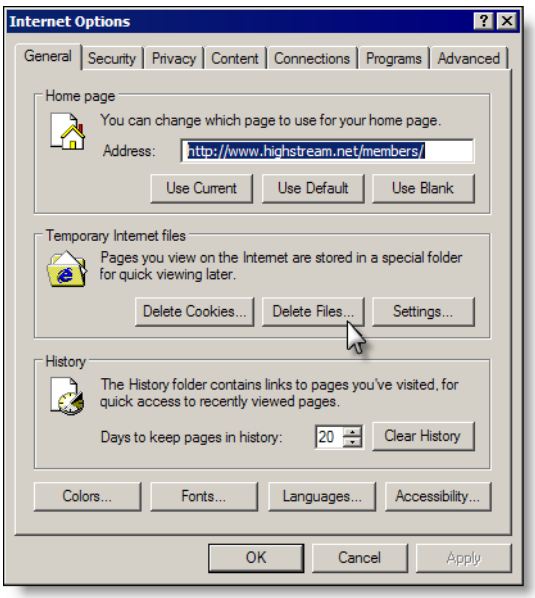
Changes to my XBuilder project do not always appear when viewed from a web browser

As you design your building control application, you will most likely compile and send your XBuilder project to the Xenta 527 at various stages of development. This allows you to verify the results of project changes as you make them.

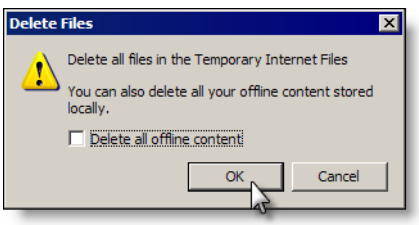
If you find that a changed web page is not displaying correctly when you view the project from a web browser, the browser may be displaying a cached version of the page. In this case, you will have to clear the web browser's temporary files in order to view the updated web page.

The following steps describe how to clear Internet Explorer's temporary files:

1 Select **Tools ▸ Internet Options** from the web browser's menu. The Internet Options dialog opens.



2 In the "Temporary Internet files" section of the dialog, click the **Delete Files...** button. This causes a confirmation dialog to open.



3 Select **OK** to delete all temporary internet files.

A network proxy/firewall is preventing the Xenta 527 from establishing proper communications.

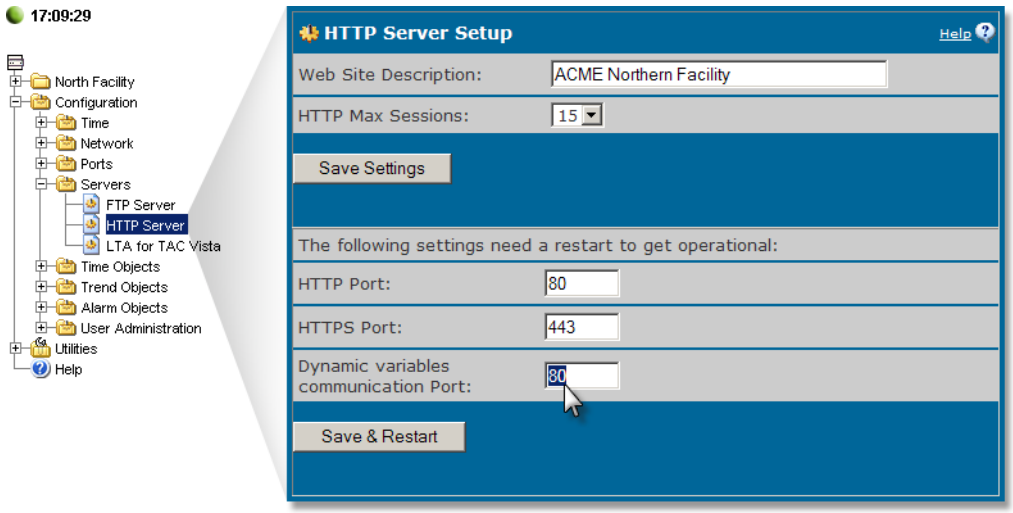
Your network configuration plays a key role in how the Xenta 527 communicates with the internet, I/NET, and Vista. If you are unable to establish proper network communications, ensure that the necessary ports are open and available to the Xenta 527. The TAC Xenta 527 uses the following communication ports:

- Port 80 (http access)
- Port 443 (https access)
- Port 20/21 (FTP access)
- Port 25 (SMTP access)
- Port 80 (Status Viewer, Alarm Viewer and Graphics Viewer)
- Port 1068 (LTA for Vista)
- Port 161 (snmp access)
- UDP Port 50069 (I/NET system access)

Perhaps you are unable to make the necessary configuration changes to your proxies/firewalls because of restrictions imposed by your company's network security policies. In this case, you have the option of choosing alternate communication ports.

The following steps describe how to use alternate communication ports:

1 Expand the navigation tree as shown in the following figure and select **HTTP Server**.



2 Set the communication port assignments to the appropriate values. Use the following fields:

- HTTP Port
- HTTPS Port
- Dynamic variables communication Port

3 Accept your settings by selecting **Save & Restart**.

4 Configure your network to allow communication on the ports you assigned to the Xenta 527.

5 Verify that the Xenta 527 can now successfully communicate across the Internet and with your building control systems.

Index

A

About this Manual 9
Access Rights 31
address, I/NET 67
alarm
  modification records 77
  point signal 69
alarm_ack, point signal 69
Alarms, I/NET 45, 77
Appendix 83
authorization level 29

B

Bit Offset object 68

C

certificate
  CA 34
  self signed 21
  SSL 34
Configuration
  Clients 36
  Instructions 15
  Profile 25
control, point signal 68
Conversion Utility 73

D

data
  limits 79
  storage 79
DCU-to-XML Conversion 39, 73
DHCP 15
DISRCFG command 36
DNS 15
Docnet 9
dynamic web pages 45

E

ENRCFG command 37
Error log
  login 32
Event Type parameter 46
Events, I/NET 45, 77
extending login time 33

F

failed logins 32
FAQs 85
Filenames 11
Find Function, using 62
Firewalls 19
Frame Settings 31
Frequently Asked Questions 85

G

Gateway 15, 19
Getting Started 13
Graphic Pages 49

H

History Logs 77
host masks 27, 85
HostNum parameter 41
HTTPS Idle TimeOut 30
Hyperterminal 15

I

I/NET
  Network 39
  Objects 67
  Point Mapping 47, 49
  Point Structure 67
  SAV Files 42, 44
  Time Schedule 58
  Trend Log 54
IP address 15, 21–22, 25

J

Java 87

K

Keystrokes 11

L

Link object 68
logging in 21

M

manual, point signal 69
Menu Commands 11

N

Network Objects 68

O

old, point signal 69

P

Packet filter 19
Page Links 69
Password 47
Point Control 69
Point object 68
point signals 68
  alarm 69
  alarm_ack 69
  control 68
  manual 69
  old 69
  test 68
  unack 69
  value 68
Point Type object 68
Points, Mapping 47, 49
ports 17, 89
Power Interruptions 79
Prerequisites 10
project
  backing up 80
  creating 40
  restoring 81
  template 40
  updating 44
Protecting Stored Data 79
Proxy Server 18

R

Reference 65
reference host 25
Remote Configuration 36

S

SAV files 42
Secure Socket Layer 33
Security 29
SSL Certificate 33
state, point 68
Station object 68
storing data 79
Subnet mask 15
system administrator 29

T

temporary files 88
Terminal Emulator 15
test, point signal 68
Time Schedule 70
Time Schedule, I/NET 58
Trend 70
Trend Log, I/NET 54
Trendlog 70
Troubleshooting 87
Typographic Conventions 10

U

unack, point signal 69
User
  Accounts 29
  Settings 30
Username parameter 47

V

value, point signal 68

W

web pages, creating 39
Web Server
  Data 79
  Security 29

X

XBuilder 67
XBuilder, using 39
XML
  Conversion Utility 73
  file 39

www.tac.com

TAC helps people feel and function better, as a direct result of greater indoor climate. This is made possible by TAC's concept of Open Systems for Building IT®, which utilizes information technology to provide clients with advantages such as indoor climate optimization, energy savings, flexibility, security, reduced expenses and user-friendly operation.

t.a.c®